SOLICITATION, OFFER AND AWARD

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE	OF	PAGES

2. CONTRACT NUMBER	3. SOLICITATION NUMBER	4. TYPE OF SOLICITATION	5. DATE ISSUED	6. REQUISITION/PURCHASE NUMBER
47QFCA19F0025	47QFCA18R0002	☐ SEALED BID (IFB) ☒ NEGOTIATED (RFP)	May 24, 2019	

7. ISSUED BY	CODE	8. ADDRESS OFFER TO *(If other than item 7)*
GSA/FEDSIM Acquisition	Q00FB000	1800 F Street, NW, 3100 Washington, DC 20405

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder".

SOLICITATION

9. Sealed offers in original and See Section L copies for furnishings the supplies or services in the Schedule will be received at the place specified in item 8, or if hand carried, in the depository located in See TOR Cover Letter until 11:00 am *(Hour)* local time 1/15/2019 *(Date)*

CAUTION - LATE Submissions, Modifications, and Withdrawals: See Section L, Provision No. 52.214-7 or 52.215-1. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL:	A. NAME	B. TELEPHONE *(NO COLLECT CALLS)*			C. E-MAIL ADDRESS
		AREA CODE	NUMBER	EXTENSION	
	Hillary A. Marshall	202	702	6745	hillary.marshall@gsa.gov

11. TABLE OF CONTENTS

(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
☒	A	SOLICITATION/CONTRACT FORM	1	☒	I	CONTRACT CLAUSES	7
☒	B	SUPPLIES OR SERVICES AND PRICES/COSTS	8			PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
☒	C	DESCRIPTION/SPECS./WORK STATEMENT	35	☒	J	LIST OF ATTACHMENTS	2
☒	D	PACKAGING AND MARKING	1			PART IV - REPRESENTATIONS AND INSTRUCTIONS	
☒	E	INSPECTION AND ACCEPTANCE	2	☒	K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	1
☒	F	DELIVERIES OR PERFORMANCE	6				
☒	G	CONTRACT ADMINISTRATION DATA	4	☒	L	INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS	16
☒	H	SPECIAL CONTRACT REQUIREMENTS	24	☒	M	EVALUATION FACTORS FOR AWARD	5

OFFER *(Must be fully completed by offeror)*

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within 120 calendar days *(60 calendar days unless a different period is inserted by the offeror)* from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT *(See Section I, Clause No. 52.232-8)*	10 CALENDAR DAYS (%)	20 CALENDAR DAYS (%)	30 CALENDAR DAYS (%)	CALENDAR DAYS(%)

14. ACKNOWLEDGMENT OF AMENDMENTS *(The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):*	AMENDMENT NO.	DATE	AMENDMENT NO.	DATE
	Amd 1	12/14/2018	Amd 2	12/14/2018
	Amd 3	1/9/2019		

15A. NAME AND ADDRESS OF OFFEROR	CODE	FACILITY	16. NAME AND THE TITLE OF PERSON AUTHORIZED TO SIGN OFFER *(Type or print)*
ECS FEDERAL, LLC 2750 PROSPERITY AVE STE 600 FAIRFAX, VA, 22031-4312 Phone: (703) 270-1540 Fax: (703) 270-1541			Cathy Kilcoyne Vice President

15B. TELEPHONE NUMBER			15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.	17. SIGNATURE	18. OFFER DATE
AREA CODE	NUMBER	EXTENSION	☐	Cathy S. Kilcoyne Digitally signed by Cathy S. Kilcoyne Date: 2019.05.24 06:57:54 -04'00'	5/24/2019
703	270	1554			

AWARD *(To be completed by Government)*

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION
	7,733,568.0	

22. AUTHORITY FOR USING OTHER THAN FULL OPEN COMPETITION:	23. SUBMIT INVOICES TO ADDRESS SHOWN IN *(4 copies unless otherwise specified)*	ITEM
☐ 10 U.S.C. 2304 (c) ☐ 41 U.S.C. 3304(a) ( )		

24. ADMINISTERED BY *(If other than Item 7)*	25. PAYMENT WILL BE MADE BY	CODE

26. NAME OF CONTRACTING OFFICER *(Type or print)*	27. UNITED STATES OF AMERICA	28. AWARD DATE
See awarded GSA Form 300 in TOS	*(Signature of Contracting Officer)*	5/24/2019

IMPORTANT - Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

TASK ORDER

47QFCA19F0025

Continuous Diagnostics and Mitigation (CDM) Dashboard Ecosystem

in support of:

Department of Homeland Security (DHS) CDM Program

Issued to:
all contractors under the General Services Administration (GSA) Alliant 2 Large Business Multiple Award Contracts

Conducted under Federal Acquisition Regulation (FAR) 16.505

Issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street, NW (QF0B)
Washington, D.C. 20405

May 24, 2019

FEDSIM Project Number HS00964

B.1 GENERAL

The work shall be performed in accordance with all Sections of this Task Order (TO) and the contractor's Basic Contract, under which the resulting TO will be placed.

B.2 CONTRACT ACCESS FEE (CAF)

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a CAF. In accordance with the Alliant 2 Large Business base contract, the CAF shall be (b)(4) percent of the total TO value with a cap of $100,000 per year per order (when order is in excess of $13.3M per order year). This TO shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO Award (TOA).

B.3 ORDER TYPES

The contractor shall perform the effort required by this TO on a Cost-Plus-Award-Fee (CPAF) basis for:

a. Mandatory Labor CLINs 0001, 1001, 2001, 3001, 4001, and 5001.
b. Optional Labor CLINs (Cloud) 1002, 2002, 3002, 4002, and 5002.
c. Optional Labor CLINs (Operations and Maintenance) 0004, 1004, 2004, 3004, 4004, and 5004.

The contractor shall perform the effort required by this TO on a Cost Reimbursement (CR) Not to Exceed (NTE) basis for:

a. Optional CDM Dashboard Cloud Hosting CLINs 1003, 2003, 3003, 4003, and 5003.
b. Long-Distance Travel CLINs 0005, 1005, 2005, 3005, 4005, and 5005.
c. ODC CLINs 0006, 1006, 2006, 3006, 4006, and 5006.
d. CAF CLINs 0007, 1007, 2007, 3007, 4007, and 5007.
e. Optional CDM Dashboard Cloud Setup CLIN 0008.

B.4 SERVICES AND PRICES/COSTS

Long-distance travel is defined as travel over 50 miles from the Washington District of Columbia (D.C.) metropolitan area. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

CLIN	Contract Line Item Number
CPAF	Cost-Plus-Award-Fee
N/A	Not Applicable
NTE	Not-to-Exceed
O&M	Operations and Maintenance
ODC	Other Direct Cost
QTY	Quantity
SOC	Security Operating Center

B.4.1 BASE PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
0001	Labor (Tasks 1–5)	(b) (4)		

OPTIONAL CPAF LABOR CLIN FOR O&M SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
0004	Labor (Task 7)	(b) (4)		

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total NTE Price
0005	Long-Distance Travel Including Indirect Handling Rate (b) (4) ___%	NTE	(b) (4)
0006	ODCs Including Indirect Handling Rate (b) (4) ____%	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
0007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING BASE PERIOD CLINs: **$__ (b) (4)**

B.4.2 FIRST OPTION PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
1001	Labor (Tasks 1–5)	(b) (4)		

OPTIONAL CPAF LABOR CLIN FOR CLOUD SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
1002	Cloud Services (Task 6, Subtasks 1-4)	(b) (4)		

OPTIONAL COST REIMBURSEMENT CLOUD HOSTING CLIN

CLIN	Description			Total NTE Price
1003	CDM Dashboard Cloud Hosting (Task 6) Including Indirect Handling Rate _(b) (4)____%			(b) (4)

OPTIONAL CPAF LABOR CLIN for O&M SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
1004	Labor (Task 7)	(b) (4)		

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total NTE Price
1005	Long-Distance Travel Including Indirect Handling Rate (b) (4) ____%	NTE	(b) (4)
1006	ODCs Including Indirect Handling Rate (b) (4) ____%	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
1007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING FIRST OPTION PERIOD CLINs: $_(b) (4)_____

B.4.3 SECOND OPTION PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
2001	Labor (Tasks 1–5)			(b) (4)

OPTIONAL CPAF LABOR CLIN FOR CLOUD SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
2002	Cloud Services (Task 6, Subtasks 1-4)			(b) (4)

OPTIONAL COST REIMBURSEMENT CLOUD HOSTING CLIN

CLIN	Description			Total NTE Price
2003	CDM Dashboard Cloud Hosting (Task 6) Including Indirect Handling Rate (b) (4) _____%			(b) (4)

OPTIONAL CPAF LABOR CLIN FOR O&M SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
2004	Labor (Task 7)			(b) (4)

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total NTE Price
2005	Long-Distance Travel Including Indirect Handling Rate (b) (4) _____%	NTE	(b) (4)
2006	ODCs Including Indirect Handling Rate (b) (4) _____%	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
2007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING SECOND OPTION PERIOD CLINs: $__(b) (4)_

B.4.4 THIRD OPTION PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
3001	Labor (Tasks 1–5)			(b) (4)

OPTIONAL CPAF LABOR CLIN FOR CLOUD SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
3002	Cloud Services (Task 6, Subtasks 1-4)			(b) (4)

OPTIONAL COST REIMBURSEMENT CLOUD HOSTING CLIN

CLIN	Description			Total NTE Price
3003	CDM Dashboard Cloud Hosting (Task 6) Including Indirect Handling Rate _(b) (4)____%			(b) (4)

OPTIONAL CPAF LABOR CLIN FOR O&M SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
3004	Labor (Task 7)			(b) (4)

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total NTE Price
3005	Long-Distance Travel Including Indirect Handling Rate (b) (4)_____%	NTE	(b) (4)
3006	ODCs Including Indirect Handling Rate (b) (4)_____%	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
3007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING THIRD OPTION PERIOD CLINs: $_(b) (4)_____

B.4.5 FOURTH OPTION PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
4001	Labor (Tasks 1–5)	(b) (4)		

OPTIONAL CPAF LABOR CLIN FOR CLOUD SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
4002	Cloud Services (Task 6, Subtasks 1-4)	(b) (4)		

OPTIONAL COST REIMBURSEMENT CLOUD HOSTING CLIN

CLIN	Description			Total NTE Price
4003	CDM Dashboard Cloud Hosting (Task 6) Including Indirect Handling Rate (b) (4) ____%			(b) (4)

OPTIONAL CPAF LABOR CLIN FOR O&M SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
4004	Labor (Task 7)	(b) (4)		

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total NTE Price
4005	Long-Distance Travel Including Indirect Handling Rate (b) (4) _____%	NTE	(b) (4)
4006	ODCs Including Indirect Handling Rate (b) (4) ____%	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
4007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING FOURTH OPTION PERIOD CLINs: $_(b) (4)_

B.4.6 FIFTH OPTION PERIOD:

MANDATORY CPAF LABOR CLIN

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
5001	Labor (Tasks 1–5)	(b) (4)		

OPTIONAL CPAF LABOR CLIN FOR CLOUD SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
5002	Cloud Services (Task 6, Subtasks 1-4)	(b) (4)		

OPTIONAL COST REIMBURSEMENT CLOUD HOSTING CLIN

CLIN	Description			Total NTE Price
5003	CDM Dashboard Cloud Hosting (Task 6) Including Indirect Handling Rate (b) (4) ____%			(b) (4)

OPTIONAL CPAF LABOR CLIN FOR O&M SERVICES

CLIN	Description	Cost	Award Fee (b) (4)	Total CPAF
5004	Labor (Task 7)	(b) (4)		

COST REIMBURSEMENT TRAVEL and ODC CLINs

CLIN	Description		Total NTE Price
5005	Long-Distance Travel Including Indirect Handling Rate (b) (4) _____%	NTE	(b) (4)
5006	ODCs Including Indirect Handling Rate (b) (4) ____%	NTE	

CONTRACT ACCESS FEE

CLIN	Description		Total Ceiling Price
5007	Contract Access Fee	NTE	(b) (4)

TOTAL CEILING FIFTH OPTION PERIOD CLINs: $_(b) (4)

OPTIONAL COST REIMBURSEMENT CDM DASHBOARD CLOUD SETUP CLIN

CLIN	Description		Unit	Total NTE Price
0008	Base or Setup Cloud Cost (Task 6) Including Indirect Handling Rate _(b)_____%			(b) (4)

GRAND TOTAL ALL CLINs: **$_ 276,112,558 _____**

B.5 SECTION B TABLES

B.5.1 INDIRECT/MATERIAL HANDLING RATE

Long-Distance Travel and ODC costs incurred may be burdened with the contractor's indirect/material handling rate in accordance with the contractor's disclosed practices, provided that the basic contract does not prohibit the application of indirect rate(s) on these costs.

a. If no indirect/material handling rate is allowable in accordance with the contractor's disclosed practices, no indirect/material handling rate shall be applied to or reimbursed on these costs.
b. If no rate is specified in the schedule of prices above, no indirect rate shall be applied to or reimbursed on these costs.

The indirect handling rate over the term of the TO shall not exceed the rate specified in the schedule of prices above.

B.5.2 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing Alliant 2 labor categories.

B.6 INCREMENTAL FUNDING

B.6.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding in the amount of **$7,733,568** for **CLINs 0001, 0004, 0005, 0006** and **0007** is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs may be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through **August 16, 2019**, unless otherwise noted in Section B. The TO may be modified to add funds incrementally up to the maximum of **$276,112,559** over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

Incremental Funding Chart for CPAF

See **Section J, Attachment B** - Incremental Funding Chart (Excel Spreadsheet).

B.7 AWARD FEE POOL VALUE REPORTING TABLE

The Award Fee Determination Plan (AFDP) establishes award fee. See **Section J, Attachment C** – Draft Award Fee Determination Plan (Word document).

C.1 BACKGROUND

The Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) Program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. The DHS CDM Program strengthens the cybersecurity of civilian Government data and networks by providing capabilities that deliver relevant, timely, and actionable information through dashboards at the Agency and Federal levels. The CDM Program follows the Office of Management and Budget (OMB) guidance M-19-02. "Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements", which requires that DHS maintain a "fully operational Federal Dashboard to provide situational awareness of the Federal Government's overall cybersecurity posture." The use of the term "CDM Dashboard" denotes both the Agency and Federal Dashboard, unless otherwise noted. The CDM Dashboard is responsible for collecting, displaying, and reporting data collected from tools and sensors deployed at Agencies for stakeholders. The cyber landscape in which Federal agencies operate is constantly changing and dynamic. Threats to the nation's information security continue to evolve and Government leaders recognize the need for a modified approach to protecting our cyber infrastructure. The CDM Program enables DHS, along with Federal Agencies and state, local, regional, and tribal governments, with the ability to enhance and further automate their existing continuous network monitoring capabilities, correlate and analyze critical cybersecurity-related information, and enhance risk-based decision making at the Agency and Federal enterprise level. The CDM Program benefits participating agencies by helping to identify information security risks on an ongoing basis so that agencies can rapidly detect and then respond to information security events.

Congress established the CDM Program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. CDM provides Federal Agencies with capabilities and tools to identify and prioritize cybersecurity risks based on potential impacts allowing cybersecurity personnel to mitigate the most significant problems first.

The CDM Program is organized by capabilities as identified below in Figure 1: CDM Capabilities.

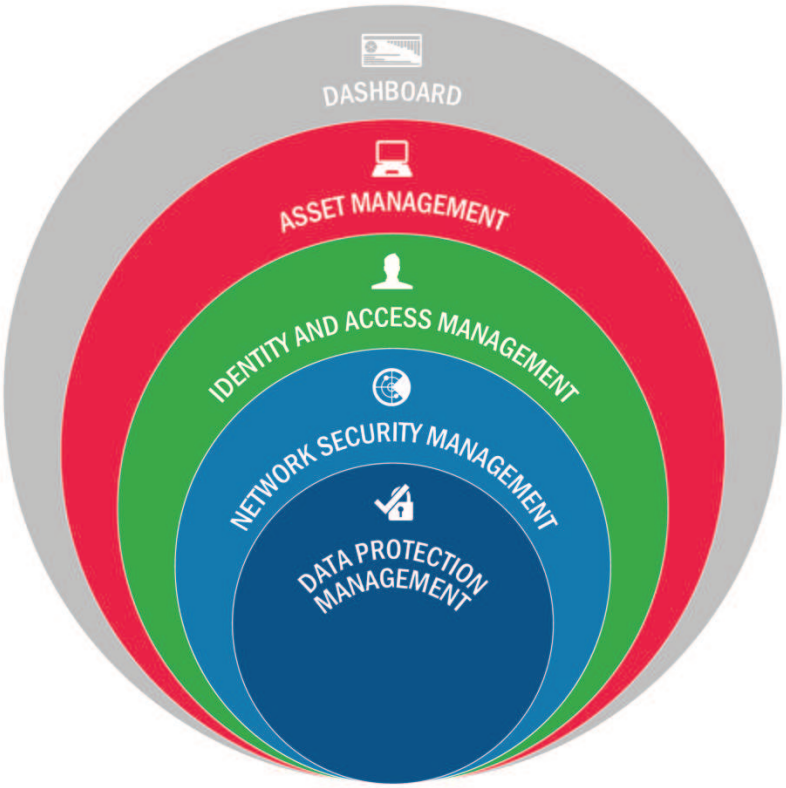

Figure 1: CDM Capabilities

The CDM Program provides cybersecurity tools, integration services, and dashboards to all participating Agencies that enable them to improve their respective security posture. The CDM Dashboards, both Federal and Agency, reinforce the CDM Program mission with an emphasis on the CDM Program's key tenant, which is to provide actionable information to allow Agencies to "fix the worst problems first" across its Information Technology (IT) networks.

The current Dashboard TO, awarded in March 2014, created a hierarchical CDM Dashboard solution. The current requirement established the Federal Dashboard, a tool that consolidates summary information from each Agency-level dashboard to form a picture of cybersecurity health across all civilian agencies. This tactical summary data (e.g., virus prevalence, use of default passwords) is used to inform strategic decision-making regarding cybersecurity risks across the Federal Government. In parallel, the CDM Program deployed Agency-level dashboards to 23 Chief Financial Officer (CFO) Act of 1990 Federal civilian agencies and will be deploying a multi-tenant dashboard to more than 40 non-CFO Act Agencies. These Agency Dashboards provide visibility of Agency computers, servers, services and other Internet-connected devices that exist either on premise or in the Agencies' virtual datacenters. This visibility, provided through its Graphical User Interface (GUI), produces customized reports, and alerts IT managers to the most critical cybersecurity risks.

C.1.1 PURPOSE

The purpose of this TO is to provide DHS with an integrated Dashboard solution for continuous monitoring and mitigation of cyber threats and vulnerabilities to the Federal .gov environment by expanding and enhancing the current instance of the Federal Dashboard through a suite of integrated hardware and software tools resulting in a "CDM Dashboard Ecosystem." The enhancement of the CDM Dashboard through this TO will provide Federal agencies with a user-friendly and intuitive solution that can be utilized to visualize and prioritize risks and vulnerabilities in an Agency's cybersecurity posture.

C.1.2 AGENCY MISSION

The CDM Program is managed within the DHS National Protection and Programs Directorate, (NPPD)/Office of Cybersecurity and Communications (CS&C)/Network Security Deployment (NSD) Division, responsible for enhancing the security, resilience, and reliability of the nation's cyber and communications infrastructure. The DHS CDM Program mission is to safeguard and secure cyberspace in an environment where the threat of cyber-attack is continuously growing and evolving. The CDM Program defends the United States (U.S.) Federal IT networks from cybersecurity threats by providing continuous monitoring sensors (tools), diagnosis, mitigation tools, and associated services to strengthen the security posture of Government networks. DHS has been given the authority and Federal funding to implement the CDM Program to ensure that the approach to continuous monitoring is consistent and meets a common set of capabilities.

C.2 SCOPE

The scope of this TO is to provide the DHS CDM Program continued enhancement and support of the CDM Dashboard for Federal Agencies as listed in this Performance Work Statement (PWS). The TO will provide a total integrated technology solution encompassing project management, project planning, iterative software development, testing and releasing of the CDM Dashboard, including Tier III services for the integrated technology solution. The migration of the CDM Dashboard to a Cloud environment and O&M services for the Federal Dashboard are included as optional tasks.

The contractor shall enter into Associate Contractor Agreements (ACAs) (**Section J, Attachment W**) with CDM integrators, e.g., Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) and TO 2F integrators, for all awarded CDM integrator TOs, and other CDM Dashboard stakeholders to ensure that CDM Dashboard requirements are coordinated properly, appropriate licenses are provided in a timely manner, ensure partnerships, and coordinate knowledge management activities (Section H.21).

C.3 CDM DASHBOARD OVERVIEW

The following subsections provide an overview of the standard CDM Architecture and CDM Dashboard guidance documents.

C.3.1 CURRENT CDM ARCHITECTURE

The current CDM architecture is developed to meet a 72-hour data currency requirement. This timeliness requirement allows the solution to facilitate near real-time reporting, triage, and

analysis of security relevant issues prevalent on an agency's network. At the Agency level, security personnel are able to immediately provide strategic return by identifying and addressing their priority vulnerabilities. Summary data from each participating Agency Dashboard is transmitted to the Federal Dashboard where the data will then be used to inform strategic decision makers regarding cybersecurity risks across the entire Federal civilian enterprise.

The current CDM system architecture, shown below in Figure 2: Current CDM Architecture, illustrates the CDM operating vision, depicted as four separate layers (i.e., Layer A, B, C, and D).

Figure 2: Current CDM Architecture

Layer A, the Tools and Sensors layer, operates on hosts and networks within agencies to collect the data from various elements of Agency information systems (e.g., hardware assets, software, users, etc.). This layer of the current CDM Architecture is the responsibility of CDM DEFEND TOs and Agency actions.

Layer B is the integration layer (collection system) that captures and collects policy-related information from Layer A in order to understand the desired security states of the information systems. This layer of the current CDM Architecture is executed through the CDM DEFEND TOs and Agency actions.

Layer C is the Agency Dashboard layer. This layer covers tasks such as risk management, ongoing authorization, metric reporting, and security operations, as well as use of automated methods called data interrogation actions, to periodically interrogate object data in order to identify system defects, gather information on Federal Information Security Management Act (FISMA) metrics, and understand the security state within an Agency. Data interrogation actions are formulated within Layers B, C, and D. The CDM Dashboard's repository within Layer C uses data interrogation actions to examine object data and to produce sets of results. These results include the detailed information about specific information system assets. Layer C dashboards also consolidate the results into summary data and make the data available to users at Layer C and Layer D. For each vulnerability identified, Layer C dashboards compute the risk score associated with each defect. This allows Agency users to prioritize which vulnerabilities to fix first. The Layer C dashboards enable users to view the results of cyber-hygiene checks, cybersecurity performance metrics, and federated queries. The development and support of the CDM Agency Dashboard is the responsibility of the contractor under this TO.

Layer D is the Federal Dashboard layer. The Federal Dashboard integrates aggregated summary data from the CDM Agency Dashboards. These customized dashboards, based on CDM Program requirements, display summary data only that enables users at Layer D to understand and track, over time, the total number of defects, .gov enterprise risk, etc. without needing to store or access the detailed Agency information. Layer D provides the mechanisms to create various elements of policy. This includes Federal data interrogation actions (e.g., defect checks, cybersecurity performance metrics, and federated queries), the Federal risk scoring algorithm, Federal risk factors (i.e., parameters of the risk scoring algorithm), and other Federal policies (e.g., configuration specifications for operating systems, the top level of the agencies organizational hierarchy, and any mandated security states). The development and support of the CDM Federal Dashboard is the responsibility of the contractor under this TO.

C.3.2 CDM DASHBOARD REQUIREMENTS

The CDM Dashboard functionality is currently governed by two documents, specifically:

a. CDM Technical Capabilities Requirements Documents, Volumes 1 and 2 (**Section J, Attachments CC and DD**): Maintained by the CDM Program Office.
b. CDM Federal Dashboard Concept of Operations (CONOPS) (July 2018): (**Section J, Attachment S**).

C.4 OBJECTIVES

The objectives of this TO are to enhance the CDM Dashboard through iterative releases to develop the CDM Dashboard Ecosystem functionality while continuing to support the current CDM Dashboard.

The achievement of these objectives will serve to:

a. Reduce Agency threat surface.
b. Increase visibility into the Federal cybersecurity posture.
c. Enhance Federal cybersecurity response capabilities.
d. Improve the CDM Dashboard's effectiveness with collection of data, display/visualization of data, aggregation of data, calculating risk indicator scores of data and reporting data.

The TO objectives align with the **CDM Dashboard Objectives** that are detailed in **Section J, Attachment HH**.

C.5 TASKS

The contractor shall perform the following tasks under the CDM Dashboard Ecosystem TO:

Task 1: Provide Project Management Services
Task 2: Conduct CDM Dashboard Project Planning
Task 3: Iteratively Develop, Test, and Release the CDM Dashboard
Task 4: Transition the CDM Dashboard to Operations
Task 5: Provide Security Accreditation, Training, and Knowledge Management Services
Task 6: Migrate and Operate the CDM Dashboard in a Cloud Environment (Optional)
Task 7: Provide Operations and Maintenance (O&M) Services for the Federal Dashboard (Optional)

C.5.1 TASK 1 – PROVIDE PROJECT MANAGEMENT SERVICES

The contractor shall provide project management services under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this PWS. The contractor shall identify a Project Manager (PM) by name that shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

The contractor shall use industry-best standards and proven methodologies that ensure all TO activities are identified, documented, and tracked so that the TO can continuously be evaluated and monitored for timely and quality service. The contractor shall notify the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer (CO) and Contracting Officer's Representative (COR) and the DHS Technical Point of Contact (TPOC) of any technical, financial, personnel, Organizational Conflict of Interest (OCI), or general managerial problems encountered throughout the TO period of performance.

C.5.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall coordinate with the FEDSIM COR to schedule, coordinate, and host a Project Kick-Off Meeting at a location approved by the Government (**Section F, Deliverable 02**). The meeting will provide an introduction between the contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues and travel/product authorization and reporting procedures. At a minimum, the attendees shall include contractor Key Personnel, representatives from DHS including the DHS TPOC, the FEDSIM CO, the FEDSIM COR, and any other Government representatives designated as a stakeholder by the Government.

At least three days prior to the Project Kick-Off Meeting, the contractor shall provide a Project Kick-Off Meeting Agenda (**Section F, Deliverable 01**) for review to the FEDSIM COR and DHS TPOC. The FEDSIM COR will approve the Project Kick-Off Meeting Agenda prior to finalizing. The Project Kick-Off Meeting Agenda shall include, at a minimum, the following topics/deliverables:

a. Introduction of Team Members and Other Personnel:
    1. Roles and responsibilities, including staffing plan and project organization.
    2. Overview of the contractor's organizational strategy to support varying locations of work and multiple Agencies.
    3. Communication Plan/Lines of communication overview (between both the contractor and Government).
    4. Draft Transition-In Plan (**Section F, Deliverable 03**) and discussion.
b. TO Management:
    1. Overview of the TO technical approach.
    2. Overview/outline of the draft Project Management Plan (PMP) (**Section F, Deliverable 04**).
    3. Overview of project tasks, schedule, and establishment of performance metrics.
    4. Identified risks and issues and applicable mitigation plans.
    5. Overview of the draft Integrated Master Schedule (IMS) (**Section F, Deliverable 05**) (shows major task, milestones, and deliverables; planned and actual start and completion dates for each).
    6. Overview of Systems Engineering Life Cycle (SELC) process as tailored to support the iterative development method.
    7. Overview of the TO draft Quality Management Plan (QMP) (**Section F, Deliverable 06**).
    8. TO logistics.
c. TO Administration:
    1. Government-Furnished Information (GFI) and Government-Furnished Property (GFP).
    2. Deliverable process and procedures.
    3. Review of Financial Status Reporting format including DHS reporting, invoice

review, and submission procedures (Section G.2).

4. Invoice Requirements.
5. Travel notification, process, and reporting.
6. Request to Initiate Purchase (RIP) submission review and approval process.
7. Security requirements/issues/facility/network access procedures.
8. Sensitivity and protection of information.
9. Reporting requirements (e.g., Monthly Status Report (MSR)).
10. Proposed reports of technical metrics on operation of the CDM Federal Dashboard as defined in the PMP.
11. Review of Draft Master Repository format (Section C.5.1.2).
12. Review of Procurement Report format.
13. Review of Problem Notification Report (PNR) process (**Section J, Attachment D**).
14. Additional administrative items including press/news releases.

The Government will provide the contractor with the number of Government participants for the Project Kick-Off Meeting and the contractor shall provide sufficient hard copies of the Project Kick-Off Meeting presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Report (**Section F, Deliverable 07**) documenting the Kick-Off Meeting discussion and capturing any action items.

C.5.1.2 SUBTASK 1.2 – MAINTAIN A MASTER REPOSITORY

The contractor shall develop and maintain a Master Repository (**Section F, Deliverable 08**) of all Travel Authorization Requests (TARs), RIPs, and deliverables. At a minimum, this repository shall include dates submitted and approved by the Government, financial information (i.e., estimated costs and costs invoiced) if applicable, pending Government actions, and any other pertinent information associated with the repository items identified above. The Master Repository is evolutionary and shall be continuously updated as requests/deliverables are submitted/responded to by the Government. The Master Repository shall be on-line/remotely accessible through standard features (e.g., web browser) to provide Government situational awareness during the TO.

The contractor shall present a Master Repository format at the Project Kick-Off Meeting for Government review. The Government will provide written approval of the proposed format via the FEDSIM COR and this approved format shall be utilized throughout the TO period of performance. The Government may request updates to the format based on CDM Program Management Office (PMO) repository requirements. The contractor shall request any changes to the format in writing to the FEDSIM COR. The contractor shall deliver all contents of the Master Repository on a quarterly basis (**Section F, Deliverable 09**) and upon Government request.

C.5.1.3 SUBTASK 1.3 – PROVIDE MSR AND CONVENE MONTHLY STATUS BRIEFING

The contractor shall develop and provide an MSR (**Section F, Deliverable 10**) via email to the DHS TPOC and the FEDSIM COR. The MSR shall briefly summarize, by task area, the TO

management and technical progress to date, as well as provide the current information indicated below. The purpose of the MSR is to ensure all stakeholders are informed of key elements of the CDM Dashboard Ecosystem project and to provide opportunities to allow stakeholder input, and coordinate resolution of risks and issues and change management, as required. The MSR shall be prepared in accordance with the MSR Template (**Section J, Attachment E**).

The contractor shall conduct a Monthly Status Briefing (**Section F, Deliverable 11**) to brief the FEDSIM COR, DHS TPOC, and other Government stakeholders on the status of the TO and activities. The Government reserves the right to change this requirement to in-person monthly status meetings, as required. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and the MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The contractor PM shall provide minutes of the Monthly Status Briefing in a Monthly Status Meeting Minutes Report (**Section F, Deliverable 12**). The Monthly Status Meeting Minutes Report shall include attendance, issues discussed, decisions made, and action items assigned. The contractor shall not conduct a Monthly Status Briefing during the same month as the Quarterly In-Progress Review (Section C.5.1.4).

The Monthly Status Briefing shall include, at a minimum:

a. The status of activities during the reported period, by task area.
b. Project schedule.
c. Financial status overview.
d. Procurement status of ODCs.
e. Status of action items, risks, and issues.
f. Progress to date on all items identified in the list above for the MSR.
g. Provide Tier III service metrics to ensure quality and timeliness in the MSR (e.g., measure quantity of tickets received and resolved; measure quality of ticket resolutions based on types of issues identified; and measure time to resolve tickets based on severity/priority).
h. Provide software development and testing metrics to ensure quality in the MSR (e.g., measure testing coverage of developed capabilities/features, measure bugs/defects detected by customers in the operational production environment, measure the time to detect bugs/defects based on type (functional bug, operational bug, security vulnerability) and measure the time to fix bugs/defects based on severity/priority).

C.5.1.4 SUBTASK 1.4 – CONDUCT QUARTERLY IN-PROGRESS REVIEW (IPR) MEETINGS

The contractor shall conduct a formal quarterly IPR (**Section F, Deliverable 14**) at a location agreed to by the Government. The IPR shall provide a forum for Government review of progress, planning, and issues related to TO performance. The contractor shall utilize the PMP in its discussion of TO performance. The IPR shall replace the Monthly Status Briefing Meeting for that month.

IPRs shall, at a minimum, include:

a. Program status overview.
b. Status of the CDM Dashboard Ecosystem development.
c. Schedule by task.
d. Previous month and quarter activities by task.
e. Planned activities for next month and quarter by task.
f. Financial status, to include quarterly cost savings report on material and equipment purchases.
g. Status of risks and issues.
h. Actions required by the Government.

The contractor shall prepare the IPR Agenda (**Section F, Deliverable 13**), IPR Meeting Report (**Section F, Deliverable 15**), and presentation material. IPRs shall be conducted no less than quarterly. For logistical planning purposes, the IPR is historically attended by an average of seven to 15 stakeholders, to include contractor personnel, FEDSIM COR, DHS TPOC, and other key Government stakeholders.

C.5.1.5 SUBTASK 1.5 – PROVIDE FINANCIAL REPORTING

The contractor shall provide a Financial Report of cumulative expenditures monthly (**Section F, Deliverable 16)** to the FEDSIM COR and DHS TPOC. The Financial Report shall include at a minimum:

a. Monthly expenditures (hours and dollars) incurred to date for each task from the start of the period of performance.
b. Projected monthly expenditures and labor hours by task starting with the current month through the end of the period of performance.
c. Funds expended, anticipated, incurred ,and remaining by CLIN.
d. Diagram reflecting funding and burn rate by month for the TO.
e. Cumulative invoiced amounts for each CLIN up to the previous month.
f. Actual current and cumulative dollars expensed for small businesses compared to Alliant 2 subcontracting goals.

The contractor shall present a Financial Report format at the Project Kick-Off Meeting (Section C.5.1.1) for Government review. The Government will provide written approval of the proposed format via the FEDSIM CO or FEDSIM COR, and this approved format shall be utilized for the monthly financial reporting requirement. The Government may request updates to the format based on DHS CDM PMO needs. Any changes to the format will be requested in writing via the FEDSIM CO or FEDSIM COR.

C.5.1.6 SUBTASK 1.6 - PROCUREMENT SERVICES, ASSET TRACKING, AND LOGISTICS

The contractor shall procure and track necessary CDM Dashboard ODCs required under the TO. The contractor shall coordinate with the FEDSIM COR and DHS TPOC and initiate the procurement of ODCs using a RIP (**Section J, Attachment M**). The contractor shall submit the RIP to the FEDSIM COR for approval prior to purchasing any ODCs. The contractor shall

develop a Procurement Report (**Section F, Deliverable 17**) in accordance with the Procurement Report Template (**Section J, Attachment II**) for CDM Dashboard ODCs procured under the TO. The Procurement Report shall initially capture the planned procurement of any CDM Dashboard ODCs, and later be updated to capture the lifecycle of Delivery and Acceptance for the CDM Dashboard ODCs. The Procurement Report shall be a living document and is anticipated to be updated periodically throughout the TO and, at a minimum, for the following instances:

a. New RIP(s).
b. Proposed cost from RIP(s), actual cost of products purchased, and price comparison, if available.
c. Cost savings to the Government (i.e., discounts).
d. Product dates of order, delivery, receipt of goods by the CDM Dashboard stakeholder.
e. The date of expiration for ODCs that require renewal.
f. Identified changes in a planned procurement of CDM Dashboard ODCs.

The contractor shall work collaboratively with the DHS TPOC and FEDSIM COR to manage property accountability, to include the acceptance of CDM Dashboard licenses.

The contractor shall identify, track, and control licenses procured under the TO and those licenses provided by the Government during the TO period of performance. The requirement to define, track, and control licenses procured under the TO shall be on-line/remotely accessible through standard features (e.g., browser) to provide Government situational awareness and ensure compliance with applicable license terms and conditions. Asset and logistics services shall include licensing inventory management and the tracking of license transfer and receipts.

The contractor shall provide associated logistical services and inventory management functions to maintain and track equipment and software accountable under this TO, including all licenses procured as part of the CDM Dashboard.

C.5.1.7 SUBTASK 1.7 – PREPARE MEETING AND TRIP REPORTS

The contractor shall conduct, attend, and participate in various project- and program-related meetings. These meetings may include, but are not limited to, Integrated Project Team (IPT) brainstorming sessions, program management reviews, technical status reviews, document reviews, and TO status reviews.

The contractor shall submit Meeting Reports (**Section F, Deliverable 18**) as requested by the FEDSIM COR and/or DHS TPOC to document meeting results and action items with owners. The Meeting Reports shall include the following information:

a. Meeting attendees and their contact information; at a minimum, identify organizations represented.
b. Meeting dates.
c. Meeting location.
d. Meeting agenda.
e. Purpose of meeting.

f. Summary of events (issues discussed, decisions made, and action items assigned).

The contractor shall submit a Trip Report (**Section F, Deliverable 19; Section J, Attachment F**). The need for a Trip Report will be identified when the TAR is submitted (**Section J, Attachment L**). The Trip Report shall include the following information:

a. Personnel traveled.
b. Dates of travel.
c. Destination(s).
d. Purpose of trip.
e. Summarized cost of the trip.
f. Approval authority.
g. Summary of events, action items, and deliverables.

C.5.1.8 SUBTASK 1.8 – PREPARE A PMP, IMS, AND QMP

Based on the contractor's proposal in response to the solicitation, the contractor shall prepare and deliver a Draft PMP (**Section F, Deliverable 04**) and a Final PMP (**Section F, Deliverable 20**).

The PMP shall contain, at a minimum, the following:

a. Management approach:
    1. Communications and stakeholder management (to include the contractor's organizational chart and lines of authority).
    2. Scope management (to include milestones, tasks, and subtasks required in this TO).
    3. Requirements management.
    4. Quality management.
    5. Configuration Management for the CDM Dashboard.
    6. Staffing management (to include the Project Staffing Plan).
    7. Procurement management.
    8. Logistics management.
    9. Cost Management.
b. Technical approach:
    1. Work Breakdown Structure (WBS) and WBS dictionary. Include associated responsibilities and partnerships between Government organizations.
    2. Risk management, including identified risks, issues, and planned mitigation.
    3. Testing.
c. Training approach.

The PMP is an evolutionary document that shall be updated annually at a minimum, and upon any alteration, modification, or adjustment to the CDM Dashboard Ecosystem solution, cost, or schedule that is sufficiently great or important and worthy of attention in the PMP. The contractor shall work from the latest Government-approved version of the PMP.

The contractor shall prepare and deliver a Draft IMS (**Section F, Deliverable 05**) and a Final IMS (**Section F, Deliverable 21)** and a Draft QMP (**Section F. Deliverable 06**) and a Final QMP (**Section F, Deliverable 22**) to accompany the PMP as separate deliverables.

The IMS is also an evolutionary document that shall be updated with technical inputs and significant changes as required. Significant changes represent any alteration, modification, or adjustment to the CDM Dashboard Ecosystem solution, cost, or schedule that is sufficiently great or important and worthy of attention in the IMS.

The contractor shall reflect the Government's requirements in planning for all activities in Tasks 2 through 5 (and optional Tasks 6 and 7, if exercised), and the tailored DHS SELC process reviews in the IMS. The contractor shall work from the latest Government-approved version of the IMS.

The QMP shall include, but not be limited to, the following:

a. Performance monitoring methods.
b. Performance measures.
c. Approach to ensure that cost, performance, and schedule comply with task planning.
d. Methodology for continuous improvement of processes and procedures, including the identification of service metrics that can be tracked in the TO.
e. Government roles.
f. Contractor roles.

The QMP is an evolutionary document that shall be updated annually at a minimum. The contractor shall work from the latest Government-approved version of the QMP.

C.5.1.9 SUBTASK 1.9 – TRANSITION-IN

The contractor shall provide transition-in services for the TO. The contractor shall conclude all transition-in activities no later than 90 calendar days after TOA.

The contractor shall provide a Draft Transition-In Plan (**Section F, Deliverable 03**) for Government approval that shall address the Tasks in Section C.5 identifying the roles and responsibilities of the contractor and incumbent, information expected from the incumbent, the process to ensure that the current CDM Dashboard activities (e.g., Tier III services) are continued without disruption, a draft schedule(s), to include the anticipated timeline for appropriate personnel security processing, and milestones to ensure no disruption of service. The contractor shall provide a Final Transition-In Plan (**Section F, Deliverable 23**) within ten business days after receipt of Government comments. The contractor shall begin transition-in activities when the Government has accepted the Final Transition-In Plan. The Final Transition-In Plan will take into account the current CDM Dashboard, which includes providing services to the CDM Federal Dashboard and the CDM Agency Dashboard instances (e.g., providing Tier III services).

The contractor shall ensure that there will be no service disruption to vital Government business and no service degradation during and after the transition-in period.

C.5.1.10 SUBTASK 1.10 - TRANSITION-OUT

The contractor shall provide transition-out services when required by the Government. The contractor shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a Draft Transition-Out Plan (**Section F, Deliverable 24**) No Later Than (NLT) 150 calendar days prior to expiration of the TO's base period and each TO option period. The contractor shall provide a Final Transition-Out Plan (**Section F, Deliverable 25**) NLT 120 calendar days prior to expiration of the TO. The contractor shall identify in the Transition-Out Plan how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

a. Project management processes.
b. Points of Contact (POCs).
c. Location of technical and project management documentation.
d. Status of ongoing technical initiatives.
e. Appropriate contractor to contractor coordination to ensure a low risk transition.
f. Transition of Key Personnel.
g. Schedules and milestones.
h. Configuration settings of all CDM Dashboard tools.
i. Asset management, including license expiration dates, where applicable.
j. Actions required of the Government.

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel during the transition-out period and shall conduct Transition-Out Status Meetings (**Section F, Deliverable 26**) no less than on a weekly basis. The contractor shall conduct Transition-Out Status Meetings more frequently, if necessary, to ensure a seamless transition-out.

The contractor shall implement its Transition-Out Plan in accordance with the Government-approved Transition-Out Plan and NLT 90 calendar days prior to expiration of the TO. All facilities, equipment, and material utilized by the contractor personnel during performance of the TO shall remain accessible to the contractor personnel during the Transition-Out period pursuant to the applicable security in-processing and out- processing guidelines.

C.5.1.11 SUBTASK 1.11 – COORDINATE AND COMPLETE SELC REVIEWS

The contractor shall coordinate and complete each SELC review detailed in the DHS SELC Process Overview (**Section J, Attachment KK**) for each CDM Dashboard release.

C.5.2 TASK 2 – CONDUCT CDM DASHBOARD PROJECT PLANNING

The contractor shall provide effective Dashboard project planning services by conducting an Analysis of Alternatives (AoA) (Section C.5.2.1) that provides in-depth analysis of topics relevant for incorporation into a future Dashboard release. In addition, the contractor shall provide a robust requirements management process, which provides traceability between varying levels of the Dashboard requirements, while providing visibility to CDM Dashboard stakeholders

of the progression of a specific Dashboard requirement from the feature backlog to actual incorporation in a Dashboard release. The CDM Dashboard Backlog (Section C.5.2.2) is provided in **Section J**, **Attachment H**. The contractor shall support the Solution Engineering Review/Project Planning Review (SER/PPR Combined Event) and Release Planning Review (RPR) SELC Gates as defined in the CDM Dashboard SELC Tailoring Guide within the SELC Process Overview (**Section J, Attachment KK**) in this task area.

C.5.2.1 SUBTASK 2.1 – DEVELOP AoA

The Government plans to analyze the CDM Agency and Federal Dashboards periodically for potential improvements, enhancements, and other changes including but not limited to the incorporation of CDM Dashboard objectives or support for a new CDM capability. To support this analysis, the contractor shall develop an AoA (**Section F, Deliverable 27**) when needed by the Government. The Government anticipates that the contractor shall complete an AoA after completing transition-in activities, and at a minimum every six months thereafter. The contractor shall provide an initial basis of estimate of labor hours and schedule to complete the AoA.

The AoA shall provide the Government with sufficient rationale on a desired topic that may affect the CDM Agency and/or Federal Dashboard. If approved for development through the release planning activities, results from the AoA may be incorporated into active development, as stated in Task 3 (Section C.5.3). Furthermore, as stated in Task 3 the contractor shall iteratively update the CDM Dashboard culminating in delivery of "potentially shippable product" or "minimum viable product" for releasing to production environment.

Individual requirements for Dashboard future releases may require a more thorough analysis than allowed during a typical release development cycle. Anticipated topics that could require the generation of an AoA include, but are not limited, to the following:

a. Incorporation of alternate architectures to best meet CDM Dashboard objectives.
b. Approach to support a new CDM Capability through the CDM Dashboard.
c. Augmentation of the existing CDM Dashboard Architecture.
d. Potential procurement of an additional Commercial Off-the-Shelf (COTS) product to be integrated into the CDM Dashboard.

The contractor shall conduct and deliver an AoA that shall include, at a minimum, the following:

a. An analysis of desired requirements and the ability for the current CDM Dashboard to support those requirements to include but not limited to technology demonstrations, modeling and simulation, and market research.
b. Identification of specific gaps in the current CDM Dashboard to support desired requirements.
c. Solutions that have the ability to meet desired requirements. Alternative solutions include, but are not limited to: additional products such as COTS and commercially supported Open Source products, architecture changes, custom development of existing CDM Dashboard.
d. Report on the cost and benefit, performance impacts, engineering trade-offs such as technical solution performance, user experience and data currency impacts, cost/benefit

analysis, schedule impacts, and technically feasible of analyzed solutions (including current CDM Dashboard).

e. Recommendation for approach to desired requirements. This shall include a rationale for the recommended approach and sound reasoning for the rejection of alternative options.

f. Summarized briefing of the recommended approach, with additional details from requirements above made available as appendices.

The AoA shall be included with a Solution Engineering Review / Project Planning Review (SER/PPR Combined Event), DHS SELC Gate Review, or as directed by the FEDSIM COR. The contractor shall deliver all required documentation to support a SER/PPR Combined Event **(Section F, Deliverable 28)** as defined in the CDM Dashboard SELC Tailoring Guide within the SELC Process Overview.

The Government will determine the best solution based on the alternatives presented in the AoA. The FEDSIM COR will coordinate and communicate with the contractor when appropriate on the next course of action after the AoA results are reported to the Government. An AoA Tracking Table is provided in **Section J, Attachment Z**.

C.5.2.2 SUBTASK 2.2 – PROVIDE REQUIREMENTS MANAGEMENT SERVICES

The contractor shall manage, elicit, analyze, document, communicate, and validate CDM Dashboard requirements while utilizing an iterative development/deployment approach. The contractor shall ensure all CDM Dashboard requirements are approved by the Government prior to development/deployment and traceable to the CDM Dashboard backlog. The contractor shall ensure that CDM Dashboard requirements are developed and refined incrementally through an iterative process of identifying needs, defining acceptance criteria, prioritizing, developing, and reviewing the results of these actions. The contractor shall ensure that the CDM Dashboard requirements management process is effectively monitored, with activity logging and traceability between requirements development and testing, which will verify and validate the Dashboard functionality is delivered to end user satisfaction.

The CDM Dashboard has a significant number of Government stakeholders and the contractor shall assist in the capture, vetting, and validation of CDM Dashboard requirements from these stakeholders and subsequently track DHS CDM PMO-approved requirements through the eventual development and release of a CDM Dashboard update.

The current CDM Dashboard Backlog catalogs the Government's desired capabilities for CDM Dashboard requirements. After TOA, the Government will provide the current CDM Dashboard Backlog to the contractor as GFI.

Upon receipt of the CDM Dashboard Backlog, the contractor shall perform the following:

a. Refine, clarify, and baseline existing and future features in the CDM Dashboard Backlog.

b. Document, clarify, and baseline existing CDM Dashboard requirements into a system that is easily accessible by CDM Dashboard stakeholders and that can manage frequent requirement related changes (adding new, modifying, removing, establishing traceability, justifications, etc.).

c. Formally baseline the existing requirements and implement a standardized process for maintaining the currency of the backlog.

The contractor shall update and maintain the CDM Dashboard Backlog **(Section F, Deliverable 29)** throughout the TO period of performance. The contractor shall include updates to the CDM Dashboard Backlog as required by the SELC activities**.**

The CDM Dashboard Backlog shall maintain traceability to CDM programmatic documents, where applicable, including the CDM Technical Capabilities Requirements Documents, Volumes 1 and 2 (**Section J, Attachments CC and DD**), and/or the CDM Federal Dashboard CONOPS (**Section J, Attachment S**).

C.5.3 TASK 3 – ITERATIVELY DEVELOP, TEST, AND RELEASE THE CDM DASHBOARD

The contractor shall iteratively develop, test, and release the CDM Dashboard. The Government will identify and prioritize CDM Dashboard capabilities in the CDM Dashboard Backlog to the contractor. The contractor shall initiate developmental activities in order to facilitate the delivery of these capabilities into an immediate, new release of the CDM Dashboard. The contractor shall follow an iterative development and testing process that incorporates consistent feedback loops with CDM Dashboard stakeholders to ensure the final release of a CDM Dashboard update encapsulates all requirements effectively. The CDM Test Team Strategy for Solution Independent Verification and Validation (IV&V) is attached in **Section J, Attachment FF**.

The contractor shall follow the CDM Dashboard SELC Process Overview that is tailored to support the iterative development approach of the CDM Dashboard. The contractor shall consistently ensure that any updates of the CDM Dashboard meet the security requirements of National Institute of Standards and Technology (NIST) and DHS security guidelines.

The Government anticipates that the CDM Dashboard shall be updated at least two times annually, commensurate with Government requirements. Each release culminates in delivery of a Beta version of software that is releasable for integration testing in a Development, Test and Evaluation (DT&E) environment and delivery of a Final version of software that is releasable to a production environment. The contractor shall support these releases by utilizing an iterative development/deployment approach and work in a team-based iterative environment with the Government CDM Dashboard Stakeholders.

For each release cycle, the contractor shall conduct testing on the CDM Federal and Agency Dashboards. The contractor shall utilize the Research, Development, Test and Evaluation (RDT&E) environment (Section C.5.3.1) to conduct testing as required, and the Government desires that industry-standard automated testing software be utilized when appropriate. The contractor's testing approach shall be consistent with the iterative development methodology.

C.5.3.1 SUBTASK 3.1 – BUILD AND MAINTAIN A RDT&E ENVIRONMENT

The contractor shall execute RDT&E activities in an environment that supports industry best practices. The RDT&E shall support research activities for future dashboard development, including supporting technology demonstrations, modeling, and simulation as part of an AoA. This includes, but is not limited to, employing tools and processes to ensure that new feature development on the CDM Dashboard, and developing updates to support existing releases to resolve issues or bugs (HotFixes) are supported in a manner that facilitates rapid application (or code) delivery for the full life cycle of delivered applications. Additionally, the contractor shall

provide RDT&E services that support interoperability testing between different releases of the dashboards to ensure baselined functionality remains stable as new releases are baselined in production environment. The RDT&E environment is intended to be the primary environment for all CDM Dashboard development. At the time of TOA, DHS will not provide access to a DHS-operated RDT&E environment.

The contractor shall provide RDT&E services that present a realistic representation of the CDM Dashboard operating environments, including Federal and Agency, which would allow for a more comprehensive method to evaluate the CDM Dashboard development. Additionally, this will enable expanded end-to-end testing capabilities to ensure proper CDM Dashboard performance and functionality exists when integrated within a full CDM Solution architecture. The contractor shall utilize simulated CDM data that is representative of expected production data of an operating CDM Solution, inclusive of data that is produced similar in quantity and structure of tools and sensors commonly deployed at Agencies.

As part of implementing best practices for a RDT&E environment, the contractor shall ensure that the following guidelines are followed as a "best effort" to represent an operational Agency:

a. RDT&E servers and workstations implementing hardening that is consistent with Government standards that are appropriate for the operating system platforms/applications.
b. Ensuring that servers and workstations that are involved with the deployment and/or testing the dashboard in the RDT&E are baselined on the latest industry available updates/patches (e.g., Operating System (OS) updates, Java Runtime Environment (JRE) updates, etc.) that are compatible with any OEM software employed in the CDM Dashboard solution.
c. Documentation of versioning of all software platforms that are relevant to the RDT&E of the CDM Dashboard solution at each test event and/or demonstration.
d. Previously released, functional CDM Dashboard platforms that are representative of what are in production environment (e.g., supported releases).

Additionally, the contractor shall share, at the request of the Government, specific configurations of the RDT&E that may be used to facilitate troubleshooting of operational deployments.

The contractor shall produce additional environments (e.g., training/test environment, demonstration sandbox) in coordination with the Government to support specific CDM Dashboard stakeholders. The Government shall have access to test or developmental environments that feature, at a minimum, the following:

a. The latest (i.e., most current) release of the CDM Dashboard hierarchy (e.g., Agency and Federal Dashboard to include information exchange capability).
b. Developmental features (e.g., Beta version of release) that are being evaluated for fulfillment in the current release.

C.5.3.2 SUBTASK 3.2 – PERFORM ITERATIVE DASHBOARD DEVELOPMENT AND TESTING OF THE CDM DASHBOARD

Before development may proceed for each release, the contractor shall work together with the Government to execute Release Planning. The Government will identify and prioritize

features/capabilities in the CDM Dashboard Backlog to the contractor, which culminates in the RPR Gate Review **(Section F, Deliverable 30).** The contractor shall deliver all required documentation to complete the RPR as defined in the CDM Dashboard SELC Process Overview (**Section J, Attachment KK**).

Following successful completion of an RPR, the contractor shall design, develop and test a Beta and Final version of software for each release cycle. The contractor shall rapidly develop prototype capabilities and demonstrate to the Government for IV&V of needs and derived requirements. The Government anticipates and prioritizes more rapid "hands on" demonstrations that occur as soon as functionally possible versus traditional one-time test events that occur later in the development timeline through Sprint Reviews and Demonstrations (SR&D).

For each release cycle, the contractor shall conduct testing on the CDM Federal and Agency Dashboards. The contractor shall identify the type and frequency of SR&D events in the Release Plan and conduct one or more SR&Ds **(Section F, Deliverable 31**), as identified by the contractor to satisfy IV&V by the Government. The intent is for the IV&V of each requirement to be attested to earlier in the development timeline. The objective of adopting a more iterative approach to customization of the CDM Dashboard platform is that the Government will emphasize more tactical, feedback driven demonstrations to supplement the traditional "gated" testing approach.

The contractor shall support Government IV&V activities, and shall assist with any additional Government operational and security-related assessments of the CDM Dashboard throughout the TO period of performance. The contractor shall allow DHS CDM PMO and/or its designated representatives (e.g., IV&V Team) to observe and/or participate in all developmental and/or operational tests and evaluations conducted by the contractor.

The contractor shall support test activities by providing Test Plans **(Section F, Deliverable 32)** and procedures, along with an environment capable of executing these plans, which outline how the contractor intends to provide evidence and/or demonstrations that targeted functionality was achieved in the release. The CDM Program Test and Evaluation Master Plan (TEMP) (**Section J, Attachment BB**) describes the CDM Program planned test and evaluation activities over the Programs' lifecycle and identifies test evaluation criteria. The contractor shall align testing activities with the CDM Program TEMP. The DHS CDM PMO and/or its designated representatives will observe and/or participate in developmental and/or operational tests and evaluations. The Government may conduct additional operational and security-related assessments of the CDM Dashboard.

For each release cycle, the contractor shall conduct testing on CDM Federal and Agency Dashboard by fulfilling the following:

a. Test cases shall be developed in the requirements management task (in accordance with Section C.5.2.2) and be available five days prior to any test event. The test cases shall include and identify, at a minimum, the following:
    1. Testing Methodologies, to include, but not limited to:
        i. Functional testing of features/capabilities.
        ii. Regression testing.
        iii. Performance testing (including stress and load tests).

iv. Security testing (including static and dynamic source code reviews) including vulnerability scans.
v. Operational assessment tests.
vi. User Acceptance testing.

2. Traceability to derived requirements.
3. Critical test parameters.
4. Evaluation criteria.

b. Schedule Test Events with clear identification of Test Cases to be evaluated during an event.
c. Document the test results following a test event in the requirements management tool, defined by the contractor.
d. Report all major issues that arise from test activities or test results that affect the schedule, and provide recommendations on how to proceed, to the DHS TPOC, FEDSIM COR, respective end-user representatives, and hosting environment representative as soon as it becomes apparent the schedule will be affected.
e. Participate in the bi-weekly Working-level Integration Product Team (WIPTs) meetings with the CDM Test team and present the status of CDM Dashboard testing activities, test artifacts, and test events.

When specifically required by the Government and/or mutually agreed to in the release plan, the contractor shall provide testing services for a formal Test Readiness Review (TRR) and conduct a formal User Acceptance Test (UAT).

When identified by the Government, the contractor shall conduct performance testing on the CDM Dashboard. Performance impact testing may not be required for each release of the CDM Dashboard. When approved by the Government, the contractor shall conduct system performance load and stress testing to ensure acceptable performance in production for the entire CDM Dashboard architecture, to include Dashboard-to-Dashboard communication and potential infrastructure considerations. To conduct the performance testing, the use of industry-standard automated testing software is strongly encouraged and the software shall be flexible to be able to handle changes and requirements of any complexity. When conducting performance testing, the contractor shall ascertain the structure and scope of a sample dataset that mimics actual agency data and develop a methodology for reproducing this dataset such that test results are relatively close to actual conditions experienced in production deployments. The contractor shall develop this methodology in conjunction with the DHS CDM PMO and seek Government approval before proceeding with the test. The contractor shall submit a System Performance Load and Stress Test Report **(Section F, Deliverable 33)** following completion of a performance test that documents results of the test event.

When identified by the Government, the contractor shall conduct end-to-end integration testing of hardware, software, and network (including Dashboard-to-Dashboard information exchange, data feeds, and application programming interface).

Following successful completion of the SR&D(s) and/or TRR/UAT, the Government will review the results of the current dashboard development increment to determine whether features/capabilities targeted for completion were implemented satisfactorily and ready for

release into production. The contractor shall conduct a Release Readiness Review (RRR) Gate Review **(Section F, Deliverable 34**). The contractor shall deliver all required documentation to complete the RRR as defined in the CDM Dashboard SELC Process Overview (**Section J, Attachment KK**) before the final version of the software can be released. The RRR will determine whether the feature/capabilities that were developed during a release meet the defined capabilities and constraints along with associated acceptance criteria and are ready to be deployed into the production environment.

C.5.3.3 SUBTASK 3.3 – DEVELOP AND RELEASE CDM DASHBOARD HOTFIXES

For each release of the CDM Dashboard to the operational production environment, the Government anticipates that one to three Quick-Fix Engineering updates or "HotFixes" will be required. HotFixes may include, but are not limited to, incorporating minor changes such as patches for the system components (e.g., the CDM Dashboard platform, messaging technology, and security patches) and/or bug fixes for information exchange with the CDM Federal Dashboard in an urgent fashion. The level-of-effort to support a HotFix is typically less than the design and development support associated with a CDM Dashboard release cycle. HotFixes will be detected and reported by a CDM Dashboard stakeholder. However, the contractor shall be prepared to proactively provide security patching for all CDM Dashboard system components when needed.

The contractor shall develop, test, and facilitate the transfer of the HotFix to CDM Dashboard stakeholders. The contractor shall update any necessary supporting documentation that is affected by a HotFix release.

C.5.4 TASK 4 – TRANSITION THE CDM DASHBOARD TO OPERATIONS

After successful completion of the Implementation and Transition to O&M RRR Gate Review, the contractor shall provide the CDM Agency Dashboard to other CDM contractors and/or the Federal Agencies where the Agency Dashboard is deployed.

The contractor shall deliver the results of the development process to the following entities for both Beta and Final CDM Dashboard releases:

a. The CDM Agency Dashboard shall be provided to each CDM DEFEND integrator, and to other CDM Dashboard stakeholders (e.g., DHS Federal Network Resilience (FNR), National Cybersecurity Center of Excellence (NCCOE), Johns Hopkins University (JHU)).
b. The CDM Federal Dashboard shall be provided only to DHS and other CDM Stakeholders (e.g., FNR, NCCOE, JHU).

The contractor shall provide Tier III services to all instances of the Agency Dashboard and to the Federal Dashboard, while utilizing Original Equipment Manufacturer (OEM) Technical Support services, as necessary, to provide in-depth technical support of CDM Dashboard issues as required.

C.5.4.1 SUBTASK 4.1 – PROVIDE TIER III SERVICES TO THE CDM DASHBOARD

The contractor shall provide Tier III services for the CDM Dashboard user community. For all operational service requests, the contractor shall establish a procedure for recording and a ticket

tracking mechanism. All requests for operational services shall be reviewed and prioritized by the DHS CDM Program Office. The contractor shall provide Tier III services during a normal work week (Monday through Friday) and provide coverage from 7:00 a.m. through 5:00 p.m. Eastern Time (ET) daily. In addition to normal working hours, the contractor shall be available during off hours to remediate escalated issues. Issues designated for escalation will be identified by the DHS TPOC, and provided to the contractor by the FEDSIM COR for remediation. While the contractor is not required to work 24 hours per day, seven days a week, 365 days per year (24x7x365), the contractor shall respond to resolve escalated issues outside normal working hours as determined by the DHS TPOC and FEDSIM COR.

The contractor shall provide Tier III services for the CDM integrators supporting the Agency CDM Dashboards (includes DEFEND integrator labs and production hosting environments) and to the Federal Dashboard. The contractor shall provide Tier III services to the DHS entity providing O&M for the Federal Dashboard. Tier III services shall include, but are not limited to, the following:

a. Provide systems engineering services necessary to establish and maintain a hot-line capability. The contractor shall refer technical issues to appropriate technical personnel and provide technical assistance.
b. Advanced engineering services to include coordination and resolution with Solution OEMs.

On a monthly basis, the contractor shall report Tier III services metrics and software development metrics to ensure quality in the MSR (Section C.5.1.3). The contractor shall, at a minimum, provide the following:

a. Measure quantity of tickets received and resolved.
b. Measure quality of ticket resolutions based on types of issues identified.
c. Measure time to resolve tickets based on severity/priority.
d. Measure testing coverage of developed capabilities/features.
e. Measure bugs/defects detected by customers in the operational production environment.
f. Measure time to detect bugs/defects based on type (functional bug, operational bug, security vulnerability).
g. Measure the time to fix bugs/defects based on severity/priority.

Tier III historical data is presented in **Section J, Attachment MM**.

C.5.4.2 SUBTASK 4.2 – PROVIDE OEM TECHNICAL SERVICES TO THE CDM DASHBOARD

The contractor shall provide OEM Field Service Technical Services as necessary to the CDM integrators supporting the Agency CDM Dashboards (includes integrator labs and production hosting environments) and to the Federal Dashboard.

Field service technical services shall include, but are not limited to:

a. Troubleshooting, analyzing, and resolving common problems related to products that compose the CDM Dashboard.

b. In-depth troubleshooting with specialized knowledge of products that compose the CDM Dashboard for remediation.
c. Advanced engineering services to include coordination and resolution with Solution OEMs.

C.5.5 TASK 5 – PROVIDE SECURITY ACCREDITATION, TRAINING, AND KNOWLEDGE MANAGEMENT

The CDM Dashboard requires additional services in areas that are complementary to the tasks described above. The subtasks addressed hereunder apply to several of the tasks above as described further below, and shall be used to support the planning, development, testing, and Tier III services of the CDM Dashboard.

C.5.5.1 SUBTASK 5.1 – PROVIDE RELEASE SECURITY ACCREDITATION SERVICES

The CDM Dashboard is a DHS asset. For each release cycle, the contractor shall update the Security Package and deliver updates to include the following documents:

a. Security Impact Assessments (SIA) (**Section F, Deliverable 35**)
b. Plan of Action and Milestones (POA&M) (**Section F, Deliverable 36**)

For major system modifications and enhancements being released that cause a significant change in the security of the system, the contractor, in close coordination with the Government, shall provide additional services, including providing updates to the existing Government-owned System Security Plan (SSP).

In addition to the above, the contractor shall perform the following security authorization tasks:

a. Provide the necessary services for security authorization and the DHS accreditation process, in accordance with DHS standards, for the CDM Federal Dashboard.
b. For Dashboard development activities, provide common/hybrid control statements for any CDM Agency Dashboard accreditation activities of CDM Federal Dashboards required (e.g., Configuration/change Management).
c. Provide developmental security/vulnerability scans to Agencies and/or CDM DEFEND integrators to enable security authorization and accreditation activities.

C.5.5.2 SUBTASK 5.2 – PROVIDE CDM DASHBOARD TRAINING

The contractor shall deliver a CDM Dashboard Training Plan **(Section F, Deliverable 37)** for the implementation and operation of the CDM Dashboard.

At a minimum, the CDM Dashboard Training Plan shall include the following:

a. Training method.
b. Training medium.
c. Training tools.
d. Frequency of training.
e. Audience.

f. Location.
g. Method to incorporate training feedback.
h. Provide integrator-specific system operation and administrator training for the CDM Dashboard.

For each release cycle, the contractor shall deliver CDM Dashboard Technical Training that covers the following:

a. Implementation instructions (e.g., release notes and installation guidance).
b. Hands-on training on how certain users can operate the delivered CDM Dashboard.
c. Content specific to the CDM Dashboard as it relates to the standardized CDM Dashboard training content with consideration of Agency unique environments.

C.5.5.3 SUBTASK 5.3 – PROVIDE KNOWLEDGE MANAGEMENT SERVICES

The contractor shall provide Knowledge Management services to support an enterprise collaborative culture as part of its web presence. The contractor shall provide services that focus on end user support to include tailoring front-end interfaces for CDM Dashboard stakeholders as well as web/portal presentation and content customization (i.e., portlets, digital authoring, and web publishing, tasking systems). The contractor shall ensure that the content management system integrates effectively with existing enterprise systems and data stores with the goal of maintaining a well-connected, secured, and controlled enterprise of systems.

C.5.6 TASK 6 – MIGRATE AND OPERATE THE CDM DASHBOARD IN A CLOUD ENVIRONMENT (OPTIONAL)

The Government does not anticipate exercising Optional Task 6 prior to the First Option Period of the TO.

At TOA, the CDM Dashboard is hosted in on-premise environments. During the execution of this TO, the Government anticipates the requirement for the contractor to migrate the CDM Dashboard capabilities to a cloud environment (e.g., Agency and/or Federal Dashboard platforms or specific capabilities thereof). Initially, cloud migration may require a hybrid approach to continue on-premises CDM Dashboards for Agencies that would potentially opt-out of a cloud approach. Upon migration, the contractor may be required to take over some/all of the O&M of the CDM Dashboard.

C.5.6.1 SUBTASK 6.1 – MIGRATE THE CDM DASHBOARD TO A CLOUD ENVIRONMENT

The contractor shall identify a Cloud Service Provider (CSP) that meets the Government's security requirements that are necessary to achieve an Authority to Operate (ATO). The contractor shall utilize security controls that meet or exceed the requirements stipulated in the Federal Risk and Authorization Management Program (FedRAMP) High baseline and/or DHS 4300A Sensitive Systems Handbook. The contractor shall prepare a Cloud AoA **(Section F, Deliverable 38)** that provides the Government with sufficient rationale for the desired selection of a specific CSP, sensitive to both performance and cost. The Cloud AoA shall include all relevant information as defined in Section C.5.2.1.

Following the selection of a CSP, the contractor shall develop and deliver a CDM Dashboard Cloud Architecture (**Section F, Deliverable 39**). The CDM Dashboard Cloud Architecture shall address, but is not limited to, the following topics:

a. Graphical representation of the Cloud configuration.
b. Networking (boundary defense, Domain Name System, Public Key Infrastructure, and Trusted Internet Connection).
c. Identity Access Management (IAM).
d. Interface architecture and specifications.
e. Data architecture and specifications.
f. Containerization and data segmentation.
g. Encryption of data storage, Data at Rest, and data in transit.
h. Multiple Tenancy.
i. Network Diagram and data flow diagram.
j. Operational Requirements.
k. Implementation and Migration Plan.

The contractor shall conduct a security assessment of the cloud environment. The Government will allow the contactor to subcontract with a Third Party Assessment Organization to conduct a security assessment if necessary. In support of the security accreditation process of the cloud environment for the CDM Dashboard, the contractor shall:

1. Provide all the required documentation for the security authorization process, including generation of a SSP (e.g., system description, system architecture, security control, etc.). This could include the following:
    a. Generation of all FedRAMP documentation, as required, to meet the FedRAMP High baseline.
    b. Generation of additional security documentation to satisfy DHS 4300a requirements.
2. Remediation of all security findings and creation of POA&Ms, as appropriate.

Following Government approval of the CDM Dashboard Cloud Architecture and after CDM Dashboard cloud environment receives its ATO, the contractor shall migrate CDM Dashboard capabilities to the cloud environment consistent with the Implementation and Migration Plan included within the Government-approved CDM Dashboard Cloud Architecture.

C.5.6.2 SUBTASK 6.2 – OPERATE, MAINTAIN, AND PROVIDE SYSTEM ADMINISTRATIVE SERVICES FOR THE CDM DASHBOARD IN THE CLOUD ENVIRONMENT

The contractor shall operate and maintain the CDM Dashboard capabilities that have been transitioned to the approved cloud environment, to include all applications/subsystems (e.g., messaging queue technology, etc.). The contractor shall also be responsible for upgrading the platform to accommodate any enhancements of existing capabilities and/or addition of new capabilities. The CDM Dashboard cloud environment operational schedule shall be 24 hours a day, seven days a week (24x7).

The contractor shall install, configure, and integrate capabilities that support each new iterative release of the CDM Dashboard. As part of the implementation of a CDM Dashboard release, the contractor shall implement the final version of software, as appropriate, in the cloud environment, to include configuration, installation, integration, account migration services, and transition to follow-on operations in production. The contractor shall conduct quality assurance and integration testing for each release to verify acceptable interoperability between the Federal and Agency Dashboards and/or their capabilities.

The contractor shall develop a Plan for Production Operations **(Section F, Deliverable 40).** The Plan for Production Operations shall describe how the contractor intends to operate the Dashboard(s). The Plan for Production Operations shall describe the O&M methodology, which includes, at a minimum:

a. Identification of requirements needed to operate the dashboard(s) through the entire life of the TO.
b. Description of detailed O&M activities that are required for successful ongoing operations, including at a minimum the following:
    1. Identification of problems and approach to fixing.
    2. Ways to improve/maintain the performance of the system.
    3. Methodology for continuously monitoring the dashboard capabilities to support implementation reviews in order to verify operational requirements are being met.
    4. Implementation of patches/HotFixes/updates for continued secure operation of the dashboard(s).
    5. Conduct scheduled and unscheduled maintenance.
    6. Identify and Maintain configuration/releases (e.g., security/patch administration).
    7. Maintain information security (e.g., security vulnerability scanning and auditing logs for suspicious behavior).
    8. Maintain Event Management (e.g., authorized service interruptions).
    9. Account Maintenance to include provisioning, disabling, and removing accounts.
    10. Methodology for measuring availability metrics (up/down).
    11. Verifying and Validating recovery processes (e.g., Backups, snapshots, and integrity thereof).
c. Approach to providing technical services for all Dashboard components and the solution as a whole, whether from a single source or multiple sources.
d. Approach to operating the CDM Dashboard(s) consistent with the system security requirements of the hosting environment.
e. Description of the configuration management and change management methodology for the Dashboard(s), to include the hosting environment, in accordance with DHS policy.

The contractor shall operate and maintain the Dashboard(s) consistent with the approved Plan for Production Operations, which include executing all activities outlined, in the manner of which they are described, in the approved plan. Additionally, the contractor shall perform as needed system administration including, but not limited to, the following types of activities:

a. Installing, configuring, and maintaining server operating systems, databases, web servers, COTS and/or commercial open-source products (supporting Section C.5.6.1).
b. Documenting virtual hardware, cloud services, system support, and/or diagnostic software, and configuration of each identified configuration item supporting a dashboard capability, for the full life cycle of the delivered capability.
c. Restoring a failed system (or data) to operational status.
d. Planning for and responding to service outages and other problems.
e. Installing system patches and upgrades.
f. Managing system resources and optimizing system performance (e.g., increasing elastic capacity of compute, memory, storage, networking bandwidth, etc.).
g. Assisting in the coordination of system downtime planned for maintenance, system patches, upgrades, or new releases.
h. Performing data and file storage administration and related functions including provisioning and monitoring backups and restorations.
i. Implementing and Maintaining any persistent data stores needed to support the dashboard(s) including:
    1. Relational/Non-Relational databases.
    2. "Big Data" technologies (e.g., Hadoop and Map Reduce).
    3. Cloud Native Document/File Repositories or Services (e.g., Amazon Web Services S3, Elastic File System, Microsoft Azure Object Storage, etc.).
j. Implementing and maintaining Identity Authentication Management (IAM) to operate, maintain, and sustain the authentication mechanism, to include Security Assertion Markup Language-based authentication services with MAX.GOV Identify Provider (IDP) (or another chosen IDP at the request of the Government).
k. Training computer operators.
l. Consulting on technical issues relating to the dashboard(s), which may be beyond the knowledge of the customer and technical staff.
m. Providing User and Account management including provisioning, modifying accesses, and de-provisioning of dashboard accounts.

The contractor shall perform problem management in coordination with the Agencies, when appropriate; to ensure that information exchange data feeds from agencies are continuously operational. The contractor shall proactively notify the Government when data communications are disrupted, as defined as any instance whereby two consecutive summary data windows are missed.

The contractor shall provide services for planning, execution, and management of data backup, Disaster Recovery (DR), and Continuity of Operations (COOP) and support as required by the Government-directed recovery point/time objective(s). Related services include, but are not limited to, ensuring data backup, DR, and COOP requirements are considered early in the application or systems' development lifecycle; verifying data backup, DR, and COOP capabilities during installation; certifying data backup, DR, and COOP compliant architectures;

creating and executing recurring data backup, DR, and COOP scenarios to test and verify continued capabilities; and reporting lessons learned and process improvements.

The contractor shall ensure the CDM Dashboard maintains its security authorization. These services may include, but are not limited, to the following:

a. Providing the necessary services for security authorization of any CDM Dashboard deployed in the approved cloud environment.
b. Providing services for the DHS and FedRAMP accreditation process in accordance with applicable DHS and/or FedRAMP standards.
c. Maintaining documentation in support of the DHS and FedRAMP accreditation process when directed.
d. Providing developmental security, vulnerability, and/or configuration scans to support security authorization and accreditation activities.

C.5.6.3 SUBTASK 6.3 – PROVIDE THE CDM DASHBOARD CLOUD ENVIRONMENT HELP DESK AND TIER I, II, AND III SERVICES

The contractor shall provide Help Desk, Tier I, II, and III services for the CDM Dashboard cloud environment. For all operational service requests, the contractor shall establish a procedure for recording and a ticket tracking mechanism. The contractor shall provide services during a normal workweek (Monday through Friday) and provide coverage from 7:00 a.m. to 5:00 p.m. ET daily. In addition to normal working hours, the contractor shall be available during off hours (24x7x365) to remediate escalated issues.

The contractor shall provide a Help Desk capability for the CDM Dashboard cloud environment. Help Desk services will include customer self-help services, online services and customer representative services supported by a “one number to call (e.g., hot-line capability).” The “one number to call (e.g., hot-line capability)” will serve as a central point of contact between the customer and the IT organization to resolve customer issues and provide a consistent and quality customer experience through the use of qualified staff, standardized processes, and an extensive knowledge management system. The Help Desk, supported by a common IT Service Management (ITSM) tool set, shall provide the ability to document, process, and monitor incidents, problems, inquiries, and change and service requests, as well as coordinate new capabilities through an actionable service catalog and support for other ITSM functions.

The contractor shall provide Tier I services for the CDM Dashboard cloud environment, which will include, but is not limited to, the following:

a. Problem resolution using standard methodologies.
b. Basic troubleshooting techniques.
c. Incident and request management.
d. Access and inventory management.
e. Change and configuration management.
f. Security and patch management consistent with the agreed to policies and procedures.

The contractor shall provide Tier II services for the CDM Dashboard cloud environment. Tier II support shall include, but is not limited to, in-depth troubleshooting with specialized knowledge of the Dashboard, or its sub-components/capabilities, for remediation.

The contractor shall provide Tier III services for the CDM Dashboard cloud environment. Tier III services shall include, but are not limited to, advanced engineering activities to include coordination and resolution with Solution OEMs.

On a monthly basis, the contractor shall report the ticket inflow to include the total number of tickets received, types of issues, and how they were resolved in the MSR (Section C.5.1.3). The contractor shall, at a minimum, provide the following services:

a. Provide initial problem resolution, where possible.
b. Generate, monitor, and track incidents through resolution, including metrics identifying time opened, time worked, time closed, and the parties' assigned responsibility through resolution.
c. Provide software support.
d. Maintain Frequently Asked Questions (FAQs) **(Section F, Deliverable 41)** and their resolutions.
e. Obtain customer feedback and conduct surveys.

C.5.6.4 SUBTASK 6.4 – PROVIDE SOC SERVICES TO THE CDM DASHBOARD CLOUD ENVIRONMENT

The contractor shall provide SOC services to CDM Dashboard cloud environment. The SOC services shall be provided in accordance with DHS 4300A Attachment F, Incident Response. SOC services shall include, but are not limited, to the following:

a. 24x7 Security Operations Center Services monitoring for all connections.
b. 24x7 Security Operations Center Services incident notifications such as up/down status.
c. Distributed Denial of Service and Availability Monitoring.
d. Integration of SIEM or SIEM equivalent capabilities to monitor environment in "real time" for active threats.
e. Triaging events to determine if an incident has occurred.
f. Coordination functions with the National Cybersecurity and Communications Integration Center/U.S.-Computer Emergency Readiness Team, and/or other external Government security staff for incident management.

C.5.7 TASK 7 – PROVIDE OPERATIONS AND MAINTENANCE (O&M) SERVICES FOR THE FEDERAL DASHBOARD (OPTIONAL)

The contractor shall provide O&M services for the Federal Dashboard. These services may be provided either from the contractor's facility or the Government site, depending on the nature of the support. The contractor may be required to work on the Government site to perform certain duties that require privileged access, e.g., system administration. The contractor shall be responsible for the complete operation, maintenance, and sustainment of the CDM Federal

Dashboard. The Government anticipates that this optional task, if needed, will be exercised soon after TO award.

C.5.7.1 SUBTASK 7.1 – OPERATE AND MAINTAIN THE CDM FEDERAL DASHBOARD

The contractor shall operate and maintain the Federal Dashboard, to include all integrated applications (e.g. messaging queue technology, etc.), Dashboard enhancements of existing capabilities and addition of new capabilities.

While DHS-designated system administrators will have access to the hosting environment **i**nfrastructure (e.g. virtualization platform, active directory, proxy, firewall), the contractor system administrators shall be responsible for the operation of the Federal Dashboard, inclusive of the RSA Archer instance, RabbitMQ messaging technology, and the addition of new capabilities.

The contractor shall install, configure, and integrate each release of the Federal Dashboard. As part of the implementation of a Federal Dashboard release, the contractor shall implement the final version of software for Federal Dashboard in the hosting environment, to include configuration, installation, integration, account migration services, and transition to follow-on operations in production. The contractor shall conduct quality assurance and technical testing for each release of the Federal Dashboard with respect to its interoperation with the information exchanges between Agency CDM Dashboards.

The contractor shall develop a Plan for Production Operations for the Federal Dashboard **(Section F, Deliverable 44).** The Plan for Production Operations for the Federal Dashboard shall describe how the contractor intends to operate the Federal Dashboard. The Plan for Production Operations for the Federal Dashboard shall describe the O&M methodology to support the Federal Dashboard, to include as a minimum:

a. Identify requirements needed to operate the Federal Dashboard through the entire life of the TO.

b. Provide a description of detailed O&M activities, including a at a minimum the following:

    1. Identification of problems and approach to fixing.
    2. Ways to improve the system,
    3. Restore a failed system to operational status
    4. Implement security patches/hot-fixes for continued secure operation of the Federal Dashboard.
    5. Conduct scheduled and unscheduled maintenance
    6. Maintain configuration/releases (e.g. security/patch administration)

7. Maintain information security (e.g. security vulnerability scanning, auditing logs for suspicious behavior)
8. Maintain Event Management (e.g. authorized service interruptions (ASIs)
9. Account Maintenance to include provisioning, disabling, and removing accounts.

c. Approach to providing technical support for all Federal Dashboard components and the solution as a whole, whether from a single source or multiple sources.

d. Approach to operating the CDM Federal Dashboard consistent with the system security requirements of the hosting environment.

e. Describe the configuration management and change management methodology for the Federal Dashboard, to include the hosting environment, is in accordance with DHS policy.

The contractor shall operate the Federal Dashboard consistent with the approved Plan for Production Operations for the Federal Dashboard. The contractor shall monitor the Federal Dashboard for system performance and functionality and elevate any issues.

The contractor shall perform problem management in coordination with the Agencies for the Federal Dashboard by identifying problems and performing resolution, to include notifying OEM vendors of application issues. The contractor shall continually monitor data feeds from Agency Dashboards, and proactively notify the government when data communications are disrupted, as defined as any instance whereby three consecutive summary data windows are missed.

The contractor shall provide support for planning, execution and management of data backup, DR, and COOP operations and support. Services include, but are not limited to, ensuring data backup, DR, and COOP requirements are considered early in the application or systems' development lifecycle; verifying data backup, DR, and COOP capabilities during installation; certifying data backup, DR, and COOP compliant architectures; creating and executing recurring data backup, DR, and COOP scenarios to test and verify continued capabilities; and reporting lessons learned and process improvements.

Periodically, the contractor shall support the Government's request to conduct implementation reviews of the Federal Dashboard in the hosting environment, which will assist the Government in measuring the Federal Dashboard's ability to meet the operational requirements, while also identifying problems, discover their causes, and recommend processes and procedures for future activities to eliminate those problems.

C.5.7.2 SUBTASK 7.2 – PROVIDE CDM DASHBOARD SYSTEM ADMINISTRATION

The contractor shall perform system administration to build, document, operate, maintain, and sustain the Federal Dashboard throughout the TO PoP. The contractor shall perform system administration and management, to include, but are not limited to:

a. Installing, configuring, and maintaining server operating systems, databases, web servers, COTS and commercial open-source products.
b. Documenting computer hardware, system support, and/or diagnostic software, and configuration settings for the full life cycle of the delivered capability.
c. Planning for and responding to service outages and other problems.
d. Installing system patches and upgrades.
e. Managing system resources and optimizing system performance.
f. Performing system startup, shutdown, diagnostics, file management, user and group setups, and determination of login scripts.
g. Assisting in the coordination of system downtime planned for maintenance, system patches, upgrades, or new releases.
h. Performing data and file storage administration and related functions including provisioning and monitoring backups and restorations.
i. Supervising or training computer operators.
j. Consulting on computer problems beyond the knowledge of the customer and technical support staff.
k. Replacement of failed components of the Federal Dashboard.

The contractor shall perform database management support, pending Agency change management approval. The contractor shall provide database management to include backup and recovery policies and procedures, database security, optimization, multi-domain operation, and performance management; support of current n-tier system on virtual machines in hosting environment or cloud infrastructure environment and migrations between these environments.

The contractor shall perform data services, and data administration services, including:

a. Data Services support includes supporting the Government with the ingestion, data tagging, and overall management of data to support a "data as a service" model.
b. Data Administration support includes, installation, organization, storage, management, administration and retrieval of data from data base management systems (DBMS); retrieval of data includes structured, semi-structured or unstructured data; database management includes relational, non-relational, or big data platforms).
c. Databases efforts will include migrations/transitions into cloud based technologies and/or creation of interfaces between classic relational databases and key indexes to cloud based columnar databases and map reduce index capabilities.

The contractor shall perform identity authentication management (IAM) to operate, maintain and sustain the authentication mechanism, to include SAML authentication services with MAX.GOV identify provider (IDP). The contractor shall provide user account provisioning for the Federal Dashboard.

C.5.7.3 SUBTASK 7.3 – PROVIDE THE CDM DASHBOARD HELP DESK, TIER I, AND TIER II SERVICES

The contractor shall provide Help Desk, Tier I, and Tier II services for the CDM Federal Dashboard. For all operational support requests, the contractor shall establish a procedure for recording and a ticket tracking mechanism. The contractor shall provide support during a normal workweek (Monday through Friday) and provide coverage from 7:00 a.m. through 5:00 p.m. ET daily. In addition to normal working hours, the contractor shall be available during off hours (365 days a year, 24 hours per day, 7 days per week) to remediate escalated issues.

The contractor shall provide Help Desk services for the Federal Dashboard. Help Desk support shall include customer self-help services, online support services and customer representative services supported by a "one number to call (e.g. hot-line capability)" as a central point of contact between the customer and the IT organization to resolve customer issues and provide a consistent and quality customer experience through the use of qualified staff, standardized processes, and an extensive knowledge management system. The Help Desk, supported by a common Information Technology Service Management (ITSM) tool set, shall provide the ability to document, process, and monitor incidents, problems, inquiries, and change and service requests, as well as coordinate new capabilities through an actionable service catalog and support for other IT service management functions. The contractor shall ensure the Government has clear visibility into all submitted tickets.

The contractor shall provide Tier I support services for the Federal Dashboard. Tier I support shall include, but is not limited to, the following:

a. Problem resolution using standard methodologies.
b. Basic troubleshooting techniques.
c. Incident and request management.
d. Access and inventory management.
e. Change and configuration management.
f. Security, and patch management consistent with the Agency's policies and procedures.

The contractor shall provide Tier II support services for the Federal Dashboard. Tier II support shall include, but is not limited to, the following:

a. In-depth troubleshooting with specialized knowledge of the Federal Dashboard for remediation;
b. All calls determined by Tier I to be related to the Federal Dashboard and not resolved through Tier I shall be forwarded to the CDM Dashboard Provider for Tier II support.

On a monthly basis, the contractor shall report the ticket inflow to include the total number of tickets received, types of issues, and how they were resolved in the MSR (Section C.5.1.3). The contractor shall, at a minimum, provide the following support:

a. Provide initial problem resolution, where possible.
b. Generate, monitor, and track incidents through resolution.
c. Provide software support.
d. Maintain FAQs for the Federal Dashboard **(Section F, Deliverable 45)** and their resolutions.
e. Obtain customer feedback and conduct surveys.

This page intentionally left blank.

E.1 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this TO will be performed by the FEDSIM COR and DHS TPOC at DHS and Agency locations in the Washington D.C. metropolitan area.

E.2 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR and DHS TPOC. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.3 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the TO and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

The final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government’s comments on deliverables shall either be incorporated in the succeeding version of the deliverable, or the contractor shall explain to the Government’s satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the quality assurance requirements stated within this TO, the document may be rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the FEDSIM COR.

E.4 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section F) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have ten workdays to incorporate the Government’s comments and/or change requests and to resubmit the deliverable in its final form.

E.5 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The FEDSIM CO/COR will provide written notification of acceptance or rejection (**Section J, Attachment G**) of all final deliverables within 15 workdays (unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.6 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies shall be corrected, by the contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the contractor does not provide products or services that conform to the ODC and CPAF requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the Award Fee Determination Report (AFDR), and there will be an associated impact to the award fee earned.

F.1 PERIOD OF PERFORMANCE

The period of performance for this TO is a 12-month base period followed by five, 12-month option periods.

Base Period:	May 24, 2019 to May 23, 2020
First Option Period:	May 24, 2020 to May 23, 2021
Second Option Period:	May 24, 2021 to May 23, 2022
Third Option Period:	May 24, 2022 to May 23, 2023
Fourth Option Period:	May 24, 2023 to May 23, 2024
Fifth Option Period:	May 24, 2024 to May 23, 2025

F.2 PLACE OF PERFORMANCE

The primary place of performance will be in the greater Washington, D.C. area with occasional travel within the Continental U.S. (CONUS) to support various stakeholder requirements. The primary place of performance will be at the contractor's site. Tier III personnel assigned to provide services under Task 4 for the Federal Dashboard, and personnel assigned to optional Task 7 personnel shall perform services at DHS facilities.

F.3 TASK ORDER SCHEDULE AND MILESTONE DATES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO.

The following abbreviations are used in this schedule:

DEL: Deliverable
NLT: No Later Than
TOA: Task Order Award
All references to days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

Data Rights Clause - Abbreviations in the Gov't Rights column of the table below shall be interpreted as follows:

UR: Unlimited Rights, per FAR 27.404-1(a) and 52.227-14

The Government asserts UR rights to open source COTS software. Any collateral agreements (within the meaning of FAR 52.227-14) proposed for data, regardless of the type of rights offered, shall be subject to the requirements of TOR Section H.14. For purposes of the foregoing, the terms "collateral agreement," "Supplier Agreement," and "Commercial Supplier Agreement" have the same meaning.

The Government does not assert any rights to management software tools if the contractor does not plan to charge the Government directly for that tool and does not propose that the Government will own or use that tool.

The contractor shall deliver the deliverables listed in the following table on the dates specified:

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
	Project Start (PS)			At TOA	N/A
01	TO Kick-Off Meeting Agenda	0001	C.5.1.1	NLT three workdays prior to the TO Kick-Off Meeting	UR
02	Kick-Off Meeting	0001	C.5.1.1	NLT 10 workdays after TOA	N/A
03	Draft Transition-In Plan	0001	C.5.1.1, C.5.1.9	TO Kick-Off Meeting	UR
04	Draft PMP	0001, X001	C.5.1.1, C.5.1.8	TO Kick-Off Meeting, and updated annually at a minimum	UR
05	Draft IMS	0001	C.5.1.1, C.5.1.8	TO Kick-Off Meeting	UR
06	Draft QMP	0001	C.5.1.1, C.5.1.8	TO Kick-Off Meeting	UR
07	Kick-Off Meeting Report	0001	C.5.1.1	NLT five days after TO Kick-Off Meeting	UR
08	Develop Master Repository	0001, X001	C.5.1.2	NLT 30 days after Government approval of format	UR
09	Master Repository Contents	0001, X001	C.5.1.2	Updated Quarterly as a Minimum	UR
10	MSR	0001, X001	C.5.1.3	Monthly, NLT 10 days after beginning of month	UR
11	Monthly Status Briefing	0001, X001	C.5.1.3	NLT 2 days after delivery of MSR	UR
12	Monthly Status Meeting Minutes Report	0001, X001	C.5.1.3	NLT 2 days after Status Briefing	UR
13	IPR Agenda	0001, X001	C.5.1.4	NLT five days prior to the IPR	UR
14	Conduct IPR	0001, X001	C.5.1.4	Quarterly	UR
15	IPR Meeting Report	0001, X001	C.5.1.4	NLT five days after the IPR	UR
16	Financial Reporting	0001, X001	C.5.1.5	Monthly	UR
17	Procurement Report	0001, X001	C.5.1.6	Updated Periodically	UR

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
18	Meeting Reports	0001, X001	C.5.1.7	As Requested, Per PMP	UR
19	Trip Report	0001, X001	C.5.1.7	NLT than 5 workdays after travel	UR
20	Final PMP	0001, X001	C.5.1.8	NLT 5 workdays after Government comment and updated at a minimum annually, or as required	UR
21	Final IMS	0001, X001	C.5.1.8	NLT 5 workdays after Government comment and updated as required	UR
22	Final QMP	0001, X001	C.5.1.8	NLT 5 workdays after Government comment and updated as required	UR
23	Final Transition-In Plan	0001	C.5.1.9	NLT than 10 days after Government comments	UR
24	Draft Transition-Out Plan	0001, X001	C.5.1.10	NLT 150 calendar days prior to the TO's Base Period and each TO option period.	UR
25	Final Transition-Out Plan	0001, X001	C.5.1.10	NLT 120 calendar days prior to expiration of the TO	UR
26	Transition-Out Status Meetings	0001, X001	C.5.1.10	No less than on a weekly basis	UR
27	Develop AoA	0001, X001	C.5.2.1	After transition-in period and at a minimum of six months thereafter	UR
28	SER and PPR Documentation	0001, X001	C.5.2.1	Per PMP	UR
29	CDM Dashboard Backlog	0001, X001	C.5.2.2	Update throughout period of performance	UR
30	RPR Gate Review	0001, X001	C.5.3.2	Per PMP	UR
31	SR&D Event	0001, X001	C.5.3.2	Per Release Plan	UR
32	Test Plan	0001, X001	C.5.3.2	Per PMP, Prior to Test	UR

DEL. #	MILESTONE/ DELIVERABLE	CLIN	TOR REFERENCE	DATE OF COMPLETION/ DELIVERY	GOV'T RIGHTS
33	Performance Load and Stress Test Report	0001, X001	C.5.3.2	After Performance Test	UR
34	RRR Gate Review	0001, X001	C.5.3.2	Per SELC, prior to final version of software	UR
35	Security Impact Assessment	0001, X001	C.5.5.1	For each release cycle	UR
36	POA&M	0001, X001	C.5.5.1	For each release cycle	UR
37	CDM Dashboard Training Plan	X001	C.5.5.2	For each release cycle	UR
38	Cloud AoA	X002x	C.5.6.1	Per PMP	UR
39	CDM Dashboard Cloud Architecture	X002x	C.5.6.1	Per PMP	UR
40	Plan for Production Operations	X002x	C.5.6.2	Per PMP	UR
41	FAQs	X002x	C.5.6.3	Per PMP	UR
42	Copy of Executed TO for Public Release	X001	F.4	NLT 10 days after date of the FEDSIM CO's execution of the initial TO, or any modification to the TO	UR
43	SCRM Plan	0001, X001	H.6.1	Per PMP	UR
44	Plan for Production Operations for the Federal Dashboard	0004, X004	C.5.7.1	Per PMP	UR
45	FAQs for the Federal Dashboard	0004, X004	C.5.7.3	Per PMP	UR
46	Acquisition Risk Questions	0001	H.6.2, L.5.2.8	Provided with Part II and updated as necesssary	N/A

The contractor shall mark all deliverables listed in the above table to indicate authorship by contractor (i.e., non-Government) personnel; provided, however, that no deliverable shall contain any proprietary markings inconsistent with the Government's data rights set forth in this TO. The Government reserves the right to treat non-conforming markings in accordance with subparagraphs (e) and (f) of the FAR clause at 52.227-14.

F.4 PUBLIC RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The contractor agrees to submit, within ten workdays from the date of the FEDSIM CO's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a Portable Document Format (PDF) file of the fully executed document with

all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA (**Section F, Deliverable 42**). The contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S. Code (U.S.C.) § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall explain why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider the contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5 DELIVERABLES MEDIA

The contractor shall deliver all electronic versions by electronic mail (email) and removable electronic media, as well as placing in the DHS' designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

a. Text	Microsoft (MS) Word, PDF
b. Spreadsheets	MS Excel
c. Briefings	MS PowerPoint
d. Drawings	MS Visio
e. Schedules	MS Project

F.6 PLACE(S) OF DELIVERY

Copies of all deliverables shall be delivered to the FEDSIM COR at the following address:

GSA FAS AAS FEDSIM
ATTN: Robert (Bob) Hibrar, COR (QF0B)
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 590-8269
Email: robert.hribar@gsa.gov

Copies of all deliverables shall also be delivered to the DHS TPOC. The DHS TPOC name, address, and contact information will be provided at award.

F.7 NOTICE REGARDING LATE DELIVERY/PNR

The contractor shall notify the FEDSIM COR via a PNR (**Section J, Attachment D**) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

G.1 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The FEDSIM CO appointed a FEDSIM COR in writing through a COR Appointment Letter (**Section J, Attachment A**). The FEDSIM COR will receive, for the Government, all work called for by the TO and will represent the FEDSIM CO in the technical phases of the work. The FEDSIM COR will provide no supervisory or instructional assistance to contractor personnel.

The FEDSIM COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the FEDSIM CO by properly executed modifications to the Contract or the TO.

G.1.1 CONTRACT ADMINISTRATION

Contracting Officer:

Melanie Pollard
GSA FAS AAS FEDSIM
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 765-7623
Email: melanie.pollard@gsa.gov

Contracting Officer's Representative:

Robert (Bob) Hibrar
GSA FAS AAS FEDSIM
1800 F Street, NW
Washington, D.C. 20405
Telephone: (202) 501-1303
Email: robert.hribar@gsa.gov

Technical Point of Contact:

Jason Neumer
DHS Cybersecurity and Inftrastructure Security Agency (CISA)
Telephone: (202) 868-7200
Email: jason.neumer@hq.dhs.gov

G.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice:

Task Order Number: *(from GSA Form 300, Block 2)*

Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*

FEDSIM Project Number: HS00964

Project Title: CDM Dashboard Ecosystem

The contractor shall submit invoices as follows:

The contractor shall utilize FEDSIM's electronic Assisted Services Shared Information SysTem (ASSIST) to submit invoices. The contractor shall manually enter CLIN charges into Central Invoice Services (CIS) in the ASSIST Portal. Summary charges on invoices shall match the charges listed in CIS for all CLINs. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Log in using your assigned ID and password, navigate to the order against which you want to invoice, click the Invoices and Acceptance Reports link in the left navigator, and then click the *Create New Invoice* button. By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. The contractor shall provide invoice backup data, as an attachment to the invoice, in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category. The FEDSIM COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment. A paper copy of the invoice is required for a credit.

The contractor is certifying, by submission of an invoice in the CIS, that the invoice is correct and proper for payment.

If there are any issues submitting an invoice, contact the Assisted Acquisition Services Business Systems (AASBS) Help Desk for support at 877-472-4877 (toll free) or by email at AASBS.helpdesk@gsa.gov.

G.3 INVOICE REQUIREMENTS

The contractor shall submit a draft copy of an invoice backup in Excel to the FEDSIM COR and DHS TPOC for review prior to its submission to ASSIST. The draft invoice shall not be construed as a proper invoice in accordance with FAR 32.9 and GSAM 532.9.

If the TO has different contract types, each shall be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion. Upon project completion, the contractor shall provide a final invoice status update monthly.

Regardless of contract type, the contractor shall report the following metadata:

a. GWAC Contract Number.
b. Task Order Award Number (NOT the Solicitation Number).
c. Contractor Invoice Number.
d. Contractor Name.
e. POC Information.
f. Current period of performance.
g. Amount of invoice that was subcontracted.

The amount of invoice that was subcontracted to a small business shall be made available upon request.

G.3.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice (all current charges shall be within the active period of performance) and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees).
b. Employee company.
c. Exempt or non-exempt designation.
d. Employee Alliant 2 labor category.
e. Current monthly and total cumulative hours worked.
f. Direct Labor Rate.
g. Effective hourly rate (e.g., cumulative costs/cumulative hours).
h. Current approved billing rate percentages in support of costs billed.
i. Itemization of cost centers applied to each individual invoiced.
j. Itemized breakout of indirect costs (e.g., Fringe, Overhead (OH), General and Administrative (G&A) burdened costs for each individual invoiced (rollups are unacceptable)).
k. Any cost incurred not billed by CLIN (e.g., lagging costs).
l. Labor adjustments from any previous months (e.g., timesheet corrections).
m. Provide comments for deviation outside of 180 hours per month per employee.

All cost presentations provided by the contractor in Excel shall show indirect charges itemized by individual with corresponding indirect rates with cost center information. The invoice detail shall be organized by CLIN.

The contractor may invoice for fee after accepting the modification which includes the award fee determination and any corresponding deobligation of unearned fee. See the AFDP in **Section J, Attachment C** for additional information on the award fee determination process.

G.3.2 OTHER DIRECT COSTS (ODCs)

The contractor may invoice monthly on the basis of cost incurred for the ODC CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

a. ODCs purchased.
b. RIP or Consent to Purchase (CTP) number or identifier.
c. Date accepted by the Government.
d. Associated CLIN.
e. Project-to-date totals by CLIN.

f. Cost incurred not billed by CLIN.
g. Remaining balance of the CLIN.

All cost presentations provided by the contractor shall also include OH charges, G&A charges and Fee in accordance with the contractor's Defense Contract Audit Agency (DCAA) cost disclosure statement.

G.3.4 TRAVEL

Contractor costs for travel will be reimbursed at the limits set in the following regulation (see FAR 31.205-46):

a. Federal Travel Regulation (FTR) - prescribed by the GSA, for travel in the contiguous U.S.

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR. The invoice shall include the period of performance covered by the invoice, the CLIN number and title. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN. The current invoice period's travel details shall include separate columns and totals and include the following:

a. TAR number or identifier, approver name, and approval date.
b. Current invoice period.
c. Names of persons traveling.
d. Number of travel days.
e. Dates of travel.
f. Number of days per diem charged.
g. Per diem rate used.
h. Total per diem charged.
i. Transportation costs.
j. Total charges.
k. Explanation of variances exceeding ten percent of the approved versus actual costs.
l. Indirect handling rate.

All cost presentations provided by the contractor shall also include OH charges and G&A charges in accordance with the contractor's DCAA cost disclosure statement.

G.4 TASK ORDER (TO) CLOSEOUT

The Government will unilaterally close out the TO no later than six years after the end of the TO period of performance if the contractor does not provide final DCAA rates by that time.

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Government does not intend to dictate the composition of the ideal team to perform this TO. The Government will evaluate up to three additional Key Personnel as proposed by the contractor. The proposed Key Personnel shall possess all required qualifications at time of proposal submission.

a. Project Manager (PM)
b. Dashboard Architect
c. Lead Dashboard Developer

The Government desires that Key Personnel be assigned for the duration of the TO. Key Personnel may be replaced or removed subject to Section H.1.4 Key Personnel Substitution.

H.1.1 PROJECT MANAGER (PM)

The contractor shall identify a PM to serve as the Government's main POC and to provide overall leadership and guidance for all contractor personnel assigned to the TO. The PM shall ultimately be responsible for the quality and efficiency of the TO. The PM shall have organizational authority to execute the requirements of the TO. The PM shall assign tasking to contractor personnel, supervise ongoing technical efforts, and manage overall TO performance to ensure the optimal use of assigned resources and subcontractors. This Key Person shall have the ultimate authority to commit the contractor's organization and make decisions for the contractor's organization in response to Government issues, concerns, or problems. The PM shall be readily available to respond to Government questions, concerns, and comments, as well as be proactive in alerting the Government to potential contractual and programmatic issues.

It is required that the PM has the following qualifications at time of proposal submission:

a. Employee of the prime contractor.
b. Possess an active Top Secret (TS) security clearance and be Sensitive Compartmented Information (SCI) eligible.

It is desirable that the PM has the following qualifications:

a. At least six years of experience managing and supervising staff and leading multi-disciplinary teams on performance-based projects similar to the CDM Dashboard Ecosystem TO.
b. At least five years of experience managing complex IT projects of similar size, scope, and complexity as identified in the TOR.
c. Knowledge and experience with the offeror's proposed methodologies and tools proposed under the CDM Dashboard Ecosystem project.
d. At least five years of experience managing teams working on system architectures, networks, and operations.
e. Current Project Management Institute (PMI) Project Management Professional or Program Management Professional certification.

H.1.2 DASHBOARD ARCHITECT

The contractor shall identify a Dashboard Architect to provide lead architecture support and systems engineering for the CDM Dashboard Ecosystem.

It is desirable that the Dashboard Architect has the following qualifications:

a. At least six years of experience designing, building, and implementing enterprise-class system architecture(s) and designing qualities into the system that match business needs (reliability, performance, maintainability, scalability, security, usability) on projects similar to the size, scope, and complexity of the work and environment described in the PWS.
b. Experience developing solutions across a diverse and heterogeneous IT environment, including the following:
    1. Technical leadership in Application development, Enterprise Architecture (EA), Service-Oriented Architecture (SOA), Integration Architecture, and IT Service Delivery to multiple U.S. Government Agencies. Additionally cloud computing experience to include scalable cloud architectures (e.g., service oriented, serverless, etc.) that aligns with mission capabilities tailored to support rapid transition and adoption across the enterprise.
    2. Experience in dashboard design using existing and emerging technologies to achieve enterprise solutions across varying environments.
    3. Experience aligning standards, frameworks, and security with overall business and technology strategy.
c. At least four years of experience serving as a lead requirements manager of a large-scale development contract tasked with the ingestion of customer requirements similar in size, scope, and complexity as described in the PWS.
d. Familiarity with the .gov Cyber Mission space and legal constraints applicable to civilian Government Agencies (e.g., SecOps, FISMA, etc.)
e. Possess a TS security clearance and be SCI eligible at time of proposal submission.

H.1.3 LEAD DASHBOARD DEVELOPER

The contractor shall identify a Lead Dashboard Developer to lead the contractor's team in the development of the CDM Dashboard.

It is desirable that the Lead Dashboard Developer has the following qualifications:

a. At least six years of experience implementing software development projects similar in size, scope, and complexity as described in the PWS.
b. Experience with dashboard development, testing, securing, integration, and implementation in a similar environment as identified in the PWS.
c. At least six years of experience designing, developing, and customizing dashboard GUI for commercial software, as well as knowledge implementing dashboard product design (user experience/user interface).
d. At least four years of experience analyzing customer requirements and providing assistance with requirements development similar in size, scope, and complexity as described in the PWS.

e. Active Certified Information Systems Security Professional (CISSP) at time of proposal submission.
f. Possess a TS security clearance and be SCI eligible at time of proposal submission.

H.1.4 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the FEDSIM CO. Prior to utilizing other than the Key Personnel specified in its proposal in response to the TOR, the contractor shall notify the FEDSIM CO and the FEDSIM COR of the existing TO. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute Key Personnel qualifications shall be equal to, or greater than, those of the Key Personnel substituted. If the FEDSIM CO and the FEDSIM COR determine that a proposed substitute Key Personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination.

H.2 RESERVED

H.3 GOVERNMENT-FURNISHED PROPERTY (GFP)

It is anticipated the Government will provide the following GFP:

a. Access to facilities, supplies, and services.
b. Access to classified and unclassified Local Area Network (LAN) services, LAN support, and telephones.

If the contractor determines additional equipment is required, the contractor shall notify the Government, in writing, of the applicable information/equipment required to accomplish the requirements.

The Government will provide access to its IT systems, including access to the current Federal Dashboard.

GFP provided to the contractor will be in accordance with FAR Part 45. This will include the use of existing IT infrastructure, consistent with the contractor's proposed technical approach.

As defined in FAR 52.245-1 (representing content as prescribed in FAR Part 45.107(a)(1)):

> All contractors employees furnished with GFP shall ensure Government barcodes are not removed. In all GFP cases, the Government retains title to the property. It is the contractor's responsibility to use GFP as it was authorized, and for the purpose intended. In the event the contractor uses Government property for other purposes without written authorization from the FEDSIM CO, the contractor may be liable for rental, without credit, of such items for each month or part of a month in which such unauthorized use occurs. The contractor shall be directly responsible and accountable for all contract property in its possession in accordance with the requirements of the TO; this also includes any contract property in the possession or control of a subcontractor.

H.4 GOVERNMENT-FURNISHED INFORMATION (GFI)

All relevant existing CDM Dashboard artifacts will be provided as GFI after TOA. The Government will provide the CDM Agency Dashboard CONOPS as GFI after TOA.

The contractor shall protect all GFI (e.g., Government data) by treating the information as Sensitive But Unclassified (SBU). SBU information and data shall only be disclosed to authorized-personnel as described in the TO herein. The contractor shall keep the information confidential and use appropriate safeguards to maintain its security in accordance with minimum Federal standards.

When no longer required, this information and data shall be returned to Government control, destroyed, or held until otherwise directed by the FEDSIM CO. The contractor shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material.

If work under this TO requires that the contractor's personnel have access to Privacy Information, contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S.C., section 552a and applicable rules and regulations.

H.5 SECURITY REQUIREMENTS

The Government requires all information pertaining to this TO be stored and protected in accordance with Government policy regarding SBU information. Therefore, no information shall be stored or transmitted outside the U.S. The information associated with this TO is critical infrastructure information as defined by 1016(e) of the U.S. Patriot Act of 2001 (42 U.S.C. 5195c(e)).

DHS security requirements are also applicable to this TO. In some instances, the contractor shall have to follow specific Agency security requirements that will be provided post-award as GFI.

H.5.1 PERSONNEL SECURITY CLEARANCES

At TOA, only the contractor's PM and contractor personnel providing Tier III support to the CDM Federal Dashboard shall be required to obtain a TS-SCI security clearance. The Government will dictate the need for any additional security clearance requirements when applicable. If optional Task 7 is exercised, all contractor personnel assigned to Task 7 shall have a TS-SCI clearance prior to working on Task 7.

In general, all necessary employee security clearances shall be at the expense of the contractor. The contractor shall comply with all security requirements.

H.5.2 DHS CONTRACTOR SECURITY REQUIREMENTS

H.5.2.1 HOMELAND SECURITY PRESIDENTIAL DIRECTIVE-12 (HSPD-12)

The contractor shall provide a list of contractor personnel that require DHS badges and security clearances. The Government will process background investigation and/or security clearances for the contractor staff to occur after submission of the staff listing, provided the individuals meet the necessary security qualifications.

H.5.2.2 POST-AWARD SECURITY REQUIREMENTS

Contractors requiring access to DHS systems (to include DHS GFP or CDM Federal Dashboard) require personnel security vetting, to include the scheduling and adjudication of the appropriate level of background investigation processed by the DHS Personnel Security Division (PSD). The DHS CDM PMO, in conjunction with the DHS PSD, shall have and exercise full control over granting, denying, withholding, or terminating unescorted Government facility and/or SBU Government information access for contractor employees, based upon the results of a background investigation. Contractor employees assigned to the TO not needing access to SBU Agency information or recurring access to Agency facilities shall not be subject to security suitability screening.

Contractor employees awaiting an Entrance on Duty (EOD) decision may begin work on the TO provided they do not access SBU Government information. Limited access to Government buildings may be allowable prior to the EOD decision if the contractor is escorted by a Government employee. This limited access is to allow contractors to attend briefings, non-recurring meetings, and begin transition work.

The contractor shall propose employees whose background offers the best prospect of obtaining a security badge approval for access. Non-U.S. citizens (foreign nationals and/or dual citizenships) are not permitted under this TO.

H.5.2.3 CONTRACTOR FITNESS DETERMINATION

The procedures outlined below shall be followed for the DHS Office of Security, PSD to process background investigations and suitability determinations, as required, in a timely and efficient manner.

Contractor employees under the TO, requiring access to sensitive information, shall be able to obtain “DHS Suitability.” The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Office of Security/PSD. Prospective contractor employees shall submit the following completed forms to the DHS Office of Security/PSD. The Standard Form 85P, “Questionnaire for Public Trust Positions” shall be completed electronically, through the Office of Personnel Management (OPM) Electronic Questionnaires for Investigations Processing (e-QIP) System. The following completed forms shall be given to the DHS Office of Security/PSD no more than three days after TOA or 30 days prior to EOD of any employees, whether a replacement, addition, subcontractor employee, or vendor:

a. Standard Form 85P, “Questionnaire for Public Trust Positions”
b. FD Form 258, “Fingerprint Card” (two copies)
c. DHS Form 11000-6 “Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement”
d. DHS Form 11000-9, “Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act”

Only complete packages will be accepted by the DHS Office of Security/PSD. Specific instructions on submission of packages will be provided upon TOA.

Failure to follow these instructions may delay the completion of suitability determinations and

background checks. Note that any delays in this process that are not caused by the Government do not relieve a contractor from performing under the terms of the TO.

DHS may, as it deems appropriate, authorize and grant a favorable EOD decision based on preliminary suitability checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow. A favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to Government facilities or information at any time during the term of the TO. No employee of the contractor shall be allowed unescorted access to a DHS facility without a favorable EOD decision or suitability determination by the DHS Office of Security/PSD.

The DHS Office of Security/PSD shall be notified of all terminations/resignations within five days of occurrence. The contractor shall return to the CDM Customer Representative all DHS-issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the CDM Customer Representative, referencing the pass or card number, name of individual to whom it was issued, and the last known location and disposition of the pass or card.

When sensitive Government information is processed on Department telecommunications and automated information systems, the contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel shall have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

DHS Security Office POC Information:

Office of Security/PSD Customer Service Support Washington, D.C. 20528

Telephone: (202) 447-5010

H.5.2.4 IT SECURITY TRAINING AND OVERSIGHT

All contractor employees accessing Government information systems, facilities, or data shall receive Security Awareness Training. This training will be provided by DHS.

Contractors who are involved with management, use, or operation of any IT systems that handle SBU information within or under the supervision of the DHS shall receive periodic training, at least annually, in security awareness and accepted security practices and systems rules of behavior. DHS contractors with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access DHS information systems shall be continually monitored while performing these duties. The contractor's PM shall be aware of any unusual or inappropriate

behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures shall be reported to the local Security Office or Information System Security Officer (ISSO).

H.5.2.5 SBU NETWORK SECURITY REQUIREMENTS

Contractor employees (to include applicants, temporaries, part-time, and replacement employees) under the TO, requiring access to SBU information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the TO. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Security Office. Prospective contractor employees shall submit the following completed forms to the DHS Security Office 30 days prior to EOD of any employees, whether a replacement, addition, or subcontractor employee:

a. Standard Form (SF) 85P, "Questionnaire for Public Trust Positions"
b. FD Form 258, "Fingerprint Card" (two copies)
c. DHS Form 11000-6, "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

DHS will provide the required forms at TOA. Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon TOA. Be advised that unless an applicant requiring access to SBU information has resided in the U.S. for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

H.5.2.6 INFORMATION ASSURANCE (IA)

This requirement implements the Government acquisition requirements pertaining to Federal policies for the security of unclassified information and information systems to the extent that those requirements apply to DHS. Contractor actions relating to information security must be in accordance with relevant Federal security statutes, regulations, guidance, and memoranda. These statutes, regulations, guidance, and memoranda include, but are not limited to, the following:

a. FISMA of 2002
b. HSPD-12
c. Clinger-Cohen Act of 1996 (40 U.S.C. 1401 et seq.)
d. Public Law 106--398, Section 1061
e. OMB Circular A-130, *Management of Federal Information Resource*
f. OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*
g. OMB M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
h. OMB M-07-18 *Implementation of Commonly Accepted Security Configurations for Windows*
i. Operating Systems (Federal Desktop Core Configuration)

j. Federal Server Core Configuration Standard
k. NIST SP to include the SP 800-18 *Guide for Developing Security Plans for Federal Information Systems*
l. NIST SP to include the SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems*
m. NIST SP to include the SP 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*
n. Federal Information Processing Standards (FIPS), to include, but not be limited to, FIPS 140-2 *Security Requirements for Cryptographic Modules*, 199, and 200

These requirements safeguard IT services provided to DHS such as the management, operation, maintenance, development, and administration of hardware, software, firmware, computer systems, networks, and telecommunications systems. Along with these Federal requirements, any solution must comply with the standards detailed within the DHS Policies, which will be made available, as needed. In addition to existing Federal standards and guidelines, it is the contractor's responsibility to adhere to new Federal standards/requirements that pertain to the security of unclassified information and information systems as these requirements are issued.

Information systems used or operated by DHS or by a contractor of DHS or other organization on behalf of the DHS must be authorized to operate by the Agency Authorizing Official (AO) through the certification and accreditation process as outlined in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. The certification process verifies that information systems have employed security controls consistent with the sensitivity of the information maintained by the system as defined by FIPS 199 and SP 800-53 and acceptably meets Federal standards such as the list of regulations identified above. During the Certification and Accreditation (C&A) process, the contractor is required to work with the Government in good faith and without question or delay to ensure that adequate mechanisms are in-place and used to protect information produced, processed, stored, and/or transmitted on or by the application.

The contractor shall provide DHS with all required documentation to support the Agency's security authorization, to include inputs to relevant portions of the Agency General Support System (GSS) SSP including descriptions of the management, operational, and technical security controls (as defined in NIST 800-53) employed in the system to the DHS TPOC and FEDSIM COR for Agency approval. This security documentation shall be prepared consistent in form and content with NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, and include any additions/augmentations described in Agency IT Policy. The security documentation shall identify and document appropriate IT security controls consistent with the sensitivity of the information and the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. The documentation shall be reviewed and updated in accordance with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* and FIPS 200 on an annual basis. Strict security requirements shall be imposed for work tasks that will be accomplished at the contractor facility which includes, but is not limited to, the following:

a. Making configuration changes to improve security (harden the application) and/or otherwise address/mitigate discovered security vulnerabilities.
b. Providing all requested information and resolve any information security vulnerabilities

identified by the Agency IA Office and/or detailed in the Security Test and Evaluation Report and/or Risk Assessment Report.

c. Documenting all system configurations in the Standard Install Process (SIP). All activities performed at contractor facilities shall comply with the following:
   1. NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems.*
   2. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems.*
   3. NISPOM, DoD Manual, DoD 5220.22-M (when applicable).

The contractor shall not co-host DHS systems with third-party sites that contain inappropriate content, which may include, but is not limited to, pornography, gambling, and political views.

The contractor shall not use DHS equipment for activities that could be considered offensive or inappropriate, including activities that may:

a. Place undue burden on Agency system components and resources.
b. Involve fundraising, non-Agency commercial purposes, non-Agency profit activities, stock trades, and gambling.
c. Result in access or transmission of objectionable material.
d. Incur additional cost to the Agency.

In addition, webmail use on the DHS equipment is strictly prohibited.

H.5.3 SECURITY SAFEGUARDS

The details of any safeguards the contractor may design or develop under this TO are the property of the Government and shall not be published or disclosed in any manner without the FEDSIM CO's express written consent.

The details of any safeguards that may be revealed to the contractor by the Government in the course of performance under the TO shall not be published or disclosed in any manner without the FEDSIM CO's express written consent.

To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the contractor shall afford the Government access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases in accordance with the FAR 52.239-1. The contractor shall use best efforts to ensure that the Government has similar access to the facilities, installations, technical capabilities, operations, documentation, records, and databases of its third-party hosting provider or sub-contractor.

If new or unanticipated IT security threats or hazards are discovered by either the Government or the contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party. Mutual agreement shall then be reached on changes or corrections to existing safeguards or institutions of new safeguards, with final determination of appropriateness being made by the Government.

H.5.4 PRIVACY CONSIDERATIONS

The Government anticipates that this TO will not involve access to privacy information,

including Sensitive Personally Identifiable Information (SPII). However, in the event that the TO results in contractor access to privacy information, then the following terms apply:

H.5.4.1 REQUIRED SECURITY AND PRIVACY TRAINING

The contractor shall provide training for all employees and subcontractors that have access to SPII as well as the creation, use, dissemination, and/or destruction of SPII, at the outset of the subcontractor's/employee's work on the TO and every year thereafter. Training shall include procedures on how to properly handle SPII, to include security requirements for transporting or transmitting SPII information, requirements for reporting a suspected breach or loss of SPII within one hour, and supporting privacy compliance and breach management activities. The contractor shall submit an email notification to the FEDSIM COR and DHS TPOC that all the contractor's employees have received privacy training prior to the beginning of the TO.

The privacy training can be obtained via Government-provided Compact Disc (CD) or through the Homeland Security Information Network at https://share.dhs.gov/nppdprivacy101training/. DHS has also published a guidebook defining SPII and setting standards for SPII handling and protection. The DHS Handbook for Safeguarding SPII is a 30-page public document on the DHS Privacy Office website.

http://www.dhs.gov/sites/default/files/publications/privacy/Guidance/handbookforsafeguardingsensitivePII_march_2012_webversion.pdf

The Management Directive for "safeguarding of SBU information" and related policies require all individuals accessing NPPD information, regardless of their employment status, be they Federal or contractor employees, to take the Information Security and Records Management Training annually. Both courses (Information Security and Records Management) can be obtained via Government-provided CD. The contractor shall maintain copies of certificates as a record of compliance. The contractor shall submit an annual email notification to the FEDSIM COR and DHS TPOC that the required Information Security, Records Management, and Privacy training has been completed for all the contractor's employees.

H.5.4.2 SUSPECTED LOSS OR COMPROMISE OF SPII (BREACH)

The contractor shall report the suspected loss or compromise of SPII by its employees or subcontractors to the DHS Help Desk at 1-800-250-7911 within one hour of the initial discovery.

The contractor shall also notify the FEDSIM CO, FEDSIM COR, and DHS TPOC via the PNR of the suspected loss or compromise. As part of the PNR, the contractor shall develop and include an Incident Response Plan, an internal system by which its employees and subcontractors are trained to identify and report potential loss or compromise of SPII. The PNR shall also include a written report within 24 hours of the suspected loss or compromise of SPII containing the following information (the written report shall also be provided to the NPPD Office of Privacy at NPPDPrivacy@hq.dhs.gov):

a. Narrative with a detailed description of the events surrounding the suspected loss/compromise.
b. Date, time, and location of the incident.
c. Type of information lost or compromised.
d. Contractor's assessment of the likelihood that the information was compromised or lost

and the reasons behind the assessment.

e. Names of person(s) involved, including victim, contractor employee/subcontractor, and any witnesses.
f. Cause of the incident and whether the company's security plan was followed or not, and which specific provisions were not followed.
g. Actions that have been or will be taken to minimize damage and/or mitigate further compromise.
h. Recommendations to prevent similar situations in the future, including whether the security plan needs to be modified in any way and whether additional training may be required.

Notwithstanding any other remedies available to NPPD, the contractor shall indemnify the NPPD against all liability (including costs and fees) for any damages arising out of violations of this requirement.

The contractor shall cooperate with NPPD or other Government Agency inquiries into the suspected loss or compromise of SPII to facilitate activities outlined in the DHS Privacy Incident Handling Guide (PIHG) and OMB M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," May 22, 2007. The DHS PIHG is an 88-page public document on the DHS Privacy Office website.

http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf

At the Government's discretion, contractor employees or subcontractor employees may be identified as no longer eligible to access SPII or to work on that TO based on their actions related to the loss or compromise of SPII.

In the event that a SPII breach occurs as a result of the violation of a term of this TO by the contractor or its employees, the contractor shall, as directed by the FEDSIM CO and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 12 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor shall be responsible for reimbursing the Government for those expenses.

H.5.5 SECURITY COMPLIANCE REQUIREMENTS

H.5.5.1 COMPLIANCE WITH DHS SECURITY POLICY

All SBU systems employed by this TO must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A, *Sensitive Systems Handbook*. All contractor systems used to process sensitive DHS data must be accredited for that use.

All national security systems produced by or supported under this TO must be compliant with DHS 4300B, *DHS National Security System Policy*.

All DHS intelligence systems produced by or supported under this TO must be compliant with DHS 4300C, *DHS Sensitive Compartmented Information (SCI) Systems Policy Directive*.

H.5.5.2 ACCESS TO UNCLASSIFIED FACILITIES, IT RESOURCES, AND SENSITIVE INFORMATION

The assurance of the security of unclassified facilities, IT resources, and sensitive information during the acquisition process and TO performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, describes how contractors must handle SBU information. DHS MD 4300.1, *Information Technology Systems Security,* and the *DHS Sensitive Systems Handbook* prescribe policies and procedures on security for IT resources. The contractor shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all TOs that require access to DHS facilities, IT resources, or sensitive information. The contractor shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the TO.

H.5.5.3 SECURITY REVIEW

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this TO are being implemented and enforced. The contractor shall afford DHS, including the organization of DHS Office of the Chief Information Officer (CIO), the Office of the Inspector General, authorized FEDSIM CO, FEDSIM COR, and other Government oversight organizations, access to the contractor's facilities, installations, operations, documentation, databases, and personnel used in the performance of this TO. The contractor will contact the DHS Chief Information Security Officer (CISO) to coordinate and participate in the review and inspection activity of Government oversight organizations external to DHS. Access shall be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS data or the function of computer systems operated on behalf of DHS and to preserve evidence of computer crime.

H.5.5.4 SECURITY REQUIREMENTS FOR UNCLASSIFIED IT RESOURCES

All unclassified IT resources shall be managed and controlled in compliance with the Department of Homeland Security Acquisition Regulation (HSAR) clause 3004.470: Security requirements for access to unclassified facilities, IT resources, and sensitive information.

H.5.5.5 CONTRACTOR EMPLOYEE ACCESS

All contractor employee access shall be managed and controlled in compliance with HSAR clause 3004.470: Security requirements for access to unclassified facilities, IT resources, and sensitive information.

H.6 SUPPLY CHAIN RISK MANAGEMENT (SCRM)

H.6.1 CONTRACTOR SAFEGUARDS

The contractor shall support supply chain protections as defined in the NIST 800-53 SA-12 control, which states, "The organization protects against supply chain threats to the information system, system component, or information system service by employing (Assignment: organization-defined security safeguards) as part of a comprehensive, defense-in-breadth

information security strategy." NIST 800-53 SA-12 can be located at the NIST website.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

The contractor shall provide the Government with an SCRM Plan (**Section F, Deliverable 43)** that describes what safeguards it intends for supply chain protections which could include only using signed software.

H.6.2 COMPANY INFORMATION REVIEW

For the purposes of supply chain risk assessment under this TO, the "organization-defined security safeguards" referenced above will include the FEDSIM CO's review of any negative findings reported by DHS as a result of the Company Information Review (CIR) conducted by DHS. The contractor is under a continuing obligation to ensure that all responses to the acquisition risk questions (**Section J, Attachment V**) answered in the CIR remain complete, accurate, and up-to-date. The contractor shall promptly notify and submit updated responses to the FEDSIM CO when any change in circumstances of the contractor or subcontractors warrants a change in the contractor's or subcontractor's responses to the acquisition risk questions. In addition, the contractor is under a continuing obligation to promptly disclose to the FEDSIM CO any proposed additional or replacement subcontractors.

H.7 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.7.1 ORGANIZATIONAL CONFLICT OF INTEREST (OCI)

a. If a contractor has performed, is currently performing work, or anticipates performing work that creates or represents an actual or potential OCI, the contractor shall immediately disclose this actual or potential OCI to the FEDSIM CO in accordance with FAR Subpart 9.5. The nature of the OCI may involve the prime contractor, subcontractors of any tier, or teaming partners.
b. The contractor is required to complete and sign an OCI Statement (**Section J, Attachment J**). The contractor must represent either that (1) It is not aware of any facts which create any actual or potential OCI relating to the award of this contract, or (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential OCI and has included a mitigation plan in accordance with paragraph (c) below.
c. If the contractor with an actual or potential OCI believes the conflict can be avoided, neutralized, or mitigated, the contractor shall submit a mitigation plan to the Government for review.
d. In addition to the mitigation plan, the FEDSIM CO may require further information from the contractor. The FEDSIM CO will use all information submitted by the contractor, and any other relevant information known to GSA, to determine whether an award to the contractor may take place, and whether the mitigation plan adequately avoids, neutralizes, or mitigates the OCI.
e. If any such conflict of interest is found to exist, the FEDSIM CO may determine that the conflict cannot be avoided, neutralized, mitigated, or otherwise resolved to the satisfaction of the Government, and the contractor may be found ineligible for award.

Alternatively, the FEDSIM CO may determine that it is otherwise in the best interest of the U.S. to contract with the contractor and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded.

f. For purposes of this procurement, the Government has determined that any company holding a CDM DEFEND task order as a prime awardee (not as a subcontractor) has an unmitigable conflict of interest and shall be ineligible to participate as a prime or subcontractor on this procurement. In addition, the prime awardee in this procurement may have an unmitigable conflict of interest for any future procurement in the CDM DEFEND series.

H.7.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an Agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) form (**Section J, Attachment K**) and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or quote information, or source selection information.
b. Are instructed in Far Part 9 for third-party disclosures when acting in an advisory capacity.

All proposed replacement contractor personnel shall also be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.8 IT ACCESSIBILITY FOR PERSONS WITH DISABILITIES

H.8.1 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 U.S.C. 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The contractor shall identify all EIT products and services provided, identify the technical standards applicable to all products and services provided, and state the degree of compliance with the applicable standards. Additionally, the contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The contractor must ensure that the list is easily accessible by typical users beginning at time of award.

a. Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220), requires that when Federal agencies develop, procure, maintain, or use Information and Communications Technology (ICT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who

have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public. All ICT that is procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this PWS shall comply with the applicable technical and functional performance criteria of the Section 508 standards unless a general exception applies.

b. When modifying commercially available or Government-owned ICT items, the contractor shall not reduce the original ICT item's level of Section 508 conformance.

c. When providing and managing hosting services for ICT items, the contractor shall ensure the hosting service does not reduce the item's original level of Section 508 conformance prior to providing the hosting service.

d. When providing installation, configuration, or integration services for ICT items, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to the services being performed.

e. When providing maintenance upgrades, substitutions, and replacements to ICT items, the contractor shall not reduce the original ICT item's level of Section 508 conformance prior to upgrade, substitution, or replacement.

f. When procuring ICT and where products that fully conform to the Section 508 standards are not commercially available, the contractor shall procure the ICT that best meets the Section 508 standards consistent with the Agency's business needs (1194, 202.7 Best Meets). When applying this standard, all procurements of ICT shall have documentation of market research that identifies which provisions cannot be met by commercially available items, and the basis for determining that the ICT to be procured best meets the Standards consistent with meeting Agency business needs as required by FAR 39.2. Any selection of a product or service that does not best meet the Revised 508 Standards due to a significant difficulty or expense shall only be permitted under an Undue Burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 139-05.

H.8.2 SECTION 508 ACCESSIBILITY STANDARDS

Revised 508 Standards: Applies to any component or portion of existing ICT purchased, developed, or altered on or after January 18, 2018, under this PWS. Text of the standards and guidelines can be found at the U.S. Access Board website.

https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the- ict-refresh/final-rule/text-of-the-standards-and-guidelines

Chapter 2: Scoping Requirements. Applies to all ICT procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this PWS.

Chapter 3: Functional Performance Criteria. Applies to all web- and non-web-based software procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this PWS that does not fully conform to Chapter 5: Software Technical Standards.

Chapter 4: Hardware Technical Standards. Applies to all hardware procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this PWS.

Chapter 5: Software Technical Standards. Applies to all web- and non-web-based software procured, modified, developed, installed, configured, integrated, deployed, maintained, and supported under this PWS.

Chapter 6: Support Documentation & Services Technical Standards. Applies to all support documentation and services under this PWS.

Original 508 Standards: Applies to any components or portion of existing ICT that has not been altered on or after January 18, 2018, under this PWS, and fully complies with the Original 508 Standards.

Section 508 Conformance Testing Methods: DHS testing methods used to validate web and non-web electronic content for conformance to the Section 508 Standards.

a. Web and Software: https://www.dhs.gov/compliance-test-processes
b. Electronic reports and documentation in MS Office or Adobe PDF format: https://www.dhs.gov/compliance-test-processes

H.8.3 SECTION 508 APPLICABLE EXCEPTIONS

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the FEDSIM COR and determination will be made in accordance with DHS MD 139-05. DHS has identified the following exceptions that may apply: E202.4 Federal Contracts, all ICT that is exclusively owned and used by the contractor to fulfill this work statement does not require conformance with the Section 508 standards. This exception does not apply to any ICT deliverable, service, or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this PWS and, for the purposes of this requirement, are not considered members of the public.

H.8.4 ACCEPTANCE CRITERIA

Prior to acceptance of ICT items that are developed, modified, or configured subject to this contract, the Government reserves the right to require the contractor to provide the following:

a. Accessibility test results based on the required test methods.
b. Documentation of features provided to help achieve accessibility and usability for people with disabilities.
c. Documentation of core functions that cannot be accessed by persons with disabilities.
d. Documentation on how to configure and install the ICT Item to support accessibility.
e. Demonstration of the ICT Item's conformance to the applicable Section 508 Standards, (including the ability of the ICT Item to create electronic content – where applicable).

H.9 ADEQUATE COST ACCOUNTING SYSTEM

The adequacy of the contractor's accounting system and its associated internal control system affect the quality and validity of the contractor data upon which the Government must rely for its

management oversight of the contractor and Contract performance. The contractor's cost accounting system shall be adequate during the entire period of performance and shall permit timely development of all necessary cost data in the form required by the Contract.

H.10 APPROVED PURCHASING SYSTEM

The objective of a contractor purchasing system assessment is to confirm it is a Government-approved purchasing system and evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting. A Government audited and approved purchasing system (e.g., approved by DCAA or Defense Contract Management Agency (DCMA)) is mandatory.

When reviews are conducted of the purchasing system during the performance of the TO, the contractor shall provide the results of the review to the FEDSIM CO within ten workdays from the date the results are known to the contractor.

H.11 TRAVEL

H.11.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulation (see FAR 31.205-46):

a. FTR - prescribed by the GSA, for travel in the contiguous U.S.

H.11.2 TARs

Three business days before undertaking travel to any Government site or any other site in performance of this TO, the contractor shall have this travel coordinated with the DHS TPOC and approved by the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long-distance travel, the contractor shall prepare a TAR (**Section J, Attachment L**) for Government review and approval. Long-distance travel will be reimbursed for cost of travel comparable with the FTR.

Requests for travel approval shall:

a. Be prepared in a legible manner.
b. Include a description of the travel proposed including a statement as to purpose.
c. Be summarized by traveler.
d. Identify the TO number.
e. Identify the CLIN associated with the travel.
f. Be submitted in advance of the travel with sufficient time to permit review and approval.

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.12 OTHER DIRECT COSTS (ODCs)

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will either be

identified at the time a TOR is issued or may be identified during the course of the TO by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO, the contractor shall submit to the FEDSIM COR a RIP (**Section J, Attachment M**). If the prime contractor is to lose an approved purchasing system, the contractor shall submit to the FEDSIM CO a CTP (**Section J, Attachment N**). Failure to possess a Government-approved purchasing system for an extended period of time after award may be grounds for contractor default. The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. Where applicable, the GSA IT Schedule 70 CDM Tool SIN cost should be used as one of the cost comparisons. The contractor shall not make any purchases without an approved RIP from the FEDSIM COR or an approved CTP from the FEDSIM CO and without complying with the requirements of Section H.14.

When the contractor submits the RIP or CTP, it shall also submit the following, when applicable:

a. A Form DD1149 (**Section J, Attachment EE**) for each group of tools, as identified by manufacturer and/or receiving Agency, that has been reviewed and signed by the receiving Agency to show concurrence.
b. A draft Form DD250 (**Section J, Attachment AA**) to match each Form DD1149 to be used upon delivery of tools as confirmation of receipt.

The contractor shall deliver the Form DD250s to the receiving Agency along with the ODCs. The receiving Agency POC will review the delivery for accuracy and show acceptance through signature on the DD250. The contractor shall email the signed DD250s to the FEDSIM COR for approval. Invoicing for procurements must have associated DD250s with the FEDSIM COR signature as supporting documentation.

H.13 ENTERPRISE ARCHITECTURE (EA) COMPLIANCE TERMS AND CONDITIONS

All DHS-funded solutions and services shall meet DHS EA (referred to as Homeland Security (HLS) EA) policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

a. All developed solutions and requirements shall be compliant with the HLS EA.
b. All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
c. Description information for all data assets, information exchanges, and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and EA Information Repository.
d. Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01, and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
e. Applicability of Internet Protocol Version 6 (IPv6) to Hosts, Routers, Systems (HRS)-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined

in the U.S. Government Version 6 (USGv6) Profile NIST SP 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

H.14 COMMERCIAL SUPPLIER AGREEMENTS

The Government understands that commercial software tools that may be purchased in furtherance of this TO as described in Section C and as contemplated in the ODC CLINs in Section B.4 (included with the final TOR) may be subject to commercial agreements which may take a variety of forms, including without limitation licensing agreements, terms of service, maintenance agreements, and the like, whether existing in hard copy or in an electronic or online format such as "clickwrap" or "browsewrap" (collectively, "Supplier Agreements"). For purposes of this TO, the Supplier Agreements are "collateral agreements" within the meaning of the FAR clause at 52.227-14.

The contractor shall ensure that any proposed Supplier Agreements allow the associated software and services to be used as necessary to achieve the objectives of this TO. The contractor shall provide all applicable Supplier Agreements to the FEDSIM CO for approval prior to purchase and shall cooperate with the Government, including negotiations with the licensor as appropriate, to ensure compliance with this section.

H.15 PRESS/NEWS RELEASE

The contractor shall not make any press/news releases pertaining to this procurement without prior Government approval and only in coordination with the FEDSIM CO.

H.16 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application, or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in FAR 52.227-14 apply.

H.17 NEW SOFTWARE

H.17.1 RIGHTS IN NEW CODE

In order to ensure that any the commercial software products or open source tools to be purchased or provided by the contractor under this TO allow the Government to meet the objectives of this TO, the contractor shall provide to the Contracting Officer, as part of the [Request to Initiate Purchase/Consent to Purchase] process, all Supplier Agreements associated with such products or tools. The Government has determined that the objectives of this TO require that the Supplier Agreements permit the creation of new code and customizations and their delivery to the Government as and when required by the Government; vest the data rights to the new code and customizations exclusively in the Government; and do not restrict Government's right and ability, directly or indirectly, to use any and all versions of the new code and customizations installed at a Government facility and to further develop and distribute them, with no further royalties or other payments being due to the contractor or any other party.

Without limiting the generality of the foregoing the Government shall have the following rights with respect to new code and customizations, at no extra charge: (a) access and use by support contractors, including a successor contractor upon termination or expiration of this TO; (b)

access and use by employees of other Federal, state, and local law enforcement agencies, as applicable; (c) transfer to a different data center and/or a successor contractor's cloud; and (d) the creation of derivative works that shall be subject to at least the same rights as set forth in subparagraphs (a) through (c) above. The above rights constitute "other rights and limitations" as contemplated in subparagraph (d) of the FAR clause at 52.227-14, Rights In Data – General (May 2014), Alternate III (Dec 2007).

If the rights to the new code and customizations are not vested in the Government upon their creation, the contractor shall assign copyright in the new code and customizations to the Government as contemplated under the FAR clause at 52.227-17, Rights in Data – Special Works (Dec 2007) upon delivery in accordance with Section F. The contractor shall provide the Government, upon request, with reasonable assistance in negotiating with the licensor to obtain the necessary changes to the Supplier Agreement. The RIP/CTP may be withheld if the required changes are not obtained.

H.17.2 DEFERRED ORDERING OF TECHNICAL DATA OR COMPUTER SOFTWARE

In addition to technical data or computer software specified elsewhere in this TO be delivered hereunder, the Government may, at any time during the performance of this TO, or within a period of three years after acceptance of all items (other than technical data or computer software) to be delivered under this TO or the termination of this TO, order any technical data or computer software generated in the performance of this TO or any subcontract hereunder. When the technical data or computer software is ordered, the contractor shall be compensated for converting the data or computer software into the prescribed form for reproduction and delivery.

The obligation to deliver the technical data of a subcontractor and pertaining to an item obtained from the contractor shall expire three years after the date the contractor accepts the last delivery of that item from that subcontractor under this TO. The Government's rights to use said data or computer software shall be pursuant to the FAR clause at 52.227-17, Rights in Data – Special Works (Dec 2007) and the clauses listed in Section H.17.3, Rights in Technical Data and Computer Software Developed Exclusively at Private Expense, of this TO.

H.17.3 RIGHTS IN TECHNICAL DATA AND COMPUTER SOFTWARE DEVELOPED EXCLUSIVELY AT PRIVATE EXPENSE

For the purposes of rights in data in the operation of this TO, the definitions, the treatment of unauthorized data markings, and the treatment of omitted markings shall be in accordance with paragraphs (a), (e), and (f), respectively, of the clause at FAR 52.227-14 in effect on the date of TOA.

To the extent that the deliverables under this TO are authorized by the Performance Work Statement (PWS) to contain either technical data or computer software developed exclusively at private expense, those data shall be subject to the Government's rights below for the specific category of data and shall be marked only in accordance with the following terms:

a. Limited Rights Technical Data. This TO may identify and specify the delivery of limited rights data, or the FEDSIM CO may require by written request the delivery of limited rights data that has been withheld or would otherwise be entitled to be withheld. If delivery of that data is required, the contractor shall affix the following "Limited Rights

Notice" to the data and the Government will treat the data, subject to the provisions of paragraphs (e) and (f) of the clause at FAR 52.227-14 in effect on the date of TOA, in accordance with the notice:

Limited Rights Notice:

a. These data are submitted with limited rights under Government Task Order No. (and subcontract, if appropriate) (TBD). These data may be reproduced and used by the Government with the express limitation that they will not, without written permission of the contractor, be used for purposes of manufacture nor disclosed outside the Government; except that the Government may disclose these data outside the Government for the following purposes, if any; provided that the Government makes such disclosure subject to prohibition against further use and disclosure:

    1. Use (except for manufacture) by support service contractors.
    2. Evaluation by non-Government evaluators.
    3. Use (except for manufacture) by other contractors participating in the Government's program of which the specific TO is a part.
    4. Emergency repair or overhaul work.
    5. Release to a foreign Government, or its instrumentalities, if required to serve the interests of the U.S. Government, for information or evaluation, or for emergency repair or overhaul work by the foreign Government.

b. This Notice shall be marked on any reproduction of these data, in whole or in part.

    1. Restricted Computer Software.

        i. This TO may identify and specify the delivery of restricted computer software, or the FEDSIM CO may require by written request the delivery of restricted computer software that has been withheld or would otherwise be entitled to be withheld. If delivery of that computer software is required, the Contractor shall affix the following "Restricted Rights Notice" to the computer software and the Government will treat the computer software, subject to paragraphs (e) and (f) of the clause at FAR 52.227-14 in effect on the date of TOA, in accordance with the notice:

Restricted Rights Notice:

a. This computer software is submitted with restricted rights under Government Task Order No. (and subcontract, if appropriate) (TBD). It may not be used, reproduced, or disclosed by the Government except as provided in paragraph (b) of this notice or as otherwise expressly stated in the Task Order.

b. This computer software may be—

    1. Used or copied for use in or with the computer(s) for which it was acquired, including use at any Government installation to which such computer(s) may be transferred;
    2. Used or copied for use in a backup computer if any computer for which it was acquired is inoperative;
    3. Reproduced for safekeeping (archives) or backup purposes;
    4. Modified, adapted, or combined with other computer software, provided that the

modified, adapted, or combined portions of the derivative software incorporating any of the delivered, restricted computer software shall be subject to the same restricted rights;

5. Disclosed to and reproduced for use by support service contractors or their subcontractors in accordance with paragraphs (b)(1) through (4) of this notice; and
6. Used or copied for use in or transferred to a replacement computer.

c. Notwithstanding the foregoing, if this computer software is copyrighted computer software, it is licensed to the Government with the minimum rights set forth in paragraph (b) of this notice.

d. Any other rights or limitations regarding the use, duplication, or disclosure of this computer software are to be expressly stated in, or incorporated in, the TO.

e. This Notice shall be marked on any reproduction of this computer software, in whole or in part.

(End of notice)

Where it is impractical to include the Restricted Rights Notice on restricted computer software, the following short-form Notice may be used instead:

Restricted Rights Notice Short Form

Use, reproduction, or disclosure is subject to restrictions set forth in TO No. 47QFCA19F0025 with ECS and its subcontractors.

(End of notice)

If restricted computer software is delivered with the copyright notice of 17 U.S.C. 401, it will be presumed to be licensed to the Government without disclosure prohibitions, with the minimum rights set forth in paragraph (b) of this clause.

(End of Clause)

H.18 AWARD FEE

See the AFDP in **Section J, Attachment C**.

H.19 STANDARDS OF CONDUCT AND RESTRICTIONS

The contractor shall conform to standards of conduct, which include the following:

a. The contractor's employees shall dress appropriately for a professional office environment while at a Government facility.

b. Contractor employees shall only conduct official business directly related to the TO while performing work under the TO.

c. Use of GFP or records for company or personal use is strictly prohibited. For example, use of Government telephones to make personal phone calls at the Government's expense is prohibited.

d. The contractor is responsible for ensuring compliance with all laws, rules, and regulations governing conduct with respect to health, safety, and use of Government property. This relates not only to the health and safety of contractor employees, but also to that of

Government personnel and other individuals.

e. Contractor employees are expected to adhere to the high professional ethical standards to which Government personnel in a comparable position would be expected to adhere. In addition, contractor employees must comply with the pertinent provisions of the Office of Federal Procurement Policy Act Amendments of 1989 and 41 U.S.C. 423.

f. The contractor shall be responsible for the actions of all personnel provided to work under this TO. In the event that damages arise from work performed by contractor-provided personnel, under the auspices of this TO, the contractor shall be responsible for all resources necessary to remedy the incident.

H.20 CONTRACTOR'S BUSINESS CONFIDENTIAL OR FINANCIAL DATA

To the extent the work under this TO requires access to business confidential or financial data of other contractors, the contractor and its employees shall protect such data from unauthorized use and disclosure and agrees not to copy or use it for any purpose other than the performance of this TO. This data may be in various forms such as documents, raw photographic prints, computer printouts, or it may be interpretative results derived from analysis, investigation, or study efforts.

The contractor shall establish policies and procedures to implement the substance of this requirement at the individual employee and subcontracting level, which will ensure that contractor, teaming partner's and subcontractor's employees are made aware of the provisions and the contractor's implementing policies and procedures. Particular attention shall be given to keeping employees advised of the statutes and regulations applicable to the handling of other contractor's confidential business or financial data, in accordance with the FAR 9.505-4.

H.21 ASSOCIATE CONTRACTOR AGREEMENT (ACA)

The contractor shall establish an ACA (**Section J, Attachment W**) with CDM Integrators, e.g., DEFEND and TO 2F, for all awarded CDM Integrator TOs, as well as any other CDM Dashboard stakeholders when directed by the Government.

I.1 TASK ORDER CLAUSES

All applicable and required clauses set forth in FAR 52.301 automatically flow down to all Alliant 2 TOs, based on their specific contract type (e.g., cost, fixed-price, etc.), PWS, competition requirements, commercial or not commercial, and dollar value as of the date the TO solicitation is issued.

I.2 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This TO incorporates one or more clauses by reference with the same force and effect as if they were given in full text. Upon request, the FEDSIM CO will make their full text available. Also, the full text of a clause may be accessed electronically at the FAR website:

http://www.acquisition.gov/far/

FAR	TITLE	DATE
52.203-13	Contractor Code of Business Ethics and Conduct	OCT 2016
52.203-14	Display of Hotline Poster(s) (fill in or provide link to client's posters)	OCT 2016
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights	APR 2014
52.204-2	Security Requirements	AUG 1996
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2016
52.204-13	System for Award Management Maintenance	OCT 2016
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-21	Basic Safeguarding of Covered Contractor Information Systems	JUN 2016
52.204-23	Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	JUL 2018
52.215-21	Requirements for Certified Cost or Pricing Data and Data Other than Certified Cost or Pricing Data—Modifications	OCT 2010
52.215-23	Limitations on Pass-Through Charges	OCT 2009
52.216-7	Allowable Cost and Payment Fill-in: 30 days	JUN 2013
52.216-8	Fixed Fee	JUN 2011
52.219-8	Utilization of Small Business Concerns	NOV 2016
52.223-16	Acquisition of EPEAT®-Registered Personal Computer Products	OCT 2015
52.224-1	Privacy Act Notification	APR 1984
52.224-2	Privacy Act	APR 1984
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008

FAR	TITLE	DATE
52.227-14	Rights in Data – General	MAY 2014
52.227-14	Rights In Data –Alternate II	DEC 2007
52.227-14	Rights In Data –Alternate III	DEC 2007
52.227-15	Representation of Limited Rights Data and Restricted Computer Software	DEC 2007
52.227-17	Rights In Data Special Works	DEC 2007
52.232-18	Availability of Funds	APR 1984
52.232-20	Limitation of Cost	APR 1984
52.232-22	Limitation of Funds	APR 1984
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.237-3	Continuity of Services	JAN 1991
52.239-1	Privacy or Security Safeguards	AUG 1996
52.244-6	Subcontracts for Commercial Items	JAN 2017
52.245-1	Government Property	JAN 2017
52.246-5	Inspection of Services—Cost-Reimbursement	APR 1984
52.246-25	Limitation of Liability – Services	FEB 1997
52.247-14	Contractor Responsibility for Receipt of Shipment	APR 1984
52.247-67	Submission of Transportation Documents for Audit Fill-in: COR, see Section G	FEB 2006
52.249-6	Termination (Cost-Reimbursement)	MAY 2004
52.249-14	Excusable Delays	APR 1984
52.251-1	Government Supply Sources	APR 2012

I.2.1 FAR CLAUSES INCORPORATED BY FULL TEXT

FAR 52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed six months. The Contracting Officer may exercise the option by written notice to the Contractor within 30 days of the end of the period of performance.

(End of clause)

FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

a. The Government may extend the term of this contract by written notice to the Contractor within 30 days; provided that the Government gives the Contractor a preliminary written

notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

b. If the Government exercises this option, the extended contract shall be considered to include this option clause.

c. The total duration of this contract, including the exercise of any options under this clause, shall not exceed 78 months.

(End of clause)

I.3 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at the GSAM website:

https://www.acquisition.gov/gsam/gsam.html/

GSAM	TITLE	DATE
552.204-9	Personal Identity Verification Requirements	OCT 2012
552.232-25	Prompt Payment	NOV 2009
552.232-39	Unenforceability of Unauthorized Obligations (FAR Deviation)	FEB 2018
552.232-78	Commercial Supplier Agreements Unenforceable Clauses	FEB 2018
552.239-70	Information Technology Security Plan and Security Authorization	JUN 2011
552.239-71	Security Requirements for Unclassified Information Technology Resources	JAN 2012

I.3.1 552.212-4 Contract Terms and Conditions—Commercial Items (FAR DEVIATION).

As prescribed in 512.301(e), replace subparagraph (g)(2), paragraph (s), and paragraph (u) of FAR clause 52.212-4. Also, add paragraph (w) to FAR clause 52.212-4.

Contract Terms and Conditions–Commercial Items (FAR DEVIATION) (Feb 2018)
(g)(2) The due date for making invoice payments by the designated payment office is the later of the following two events:

(i) The 10th day after the designated billing office receives a proper invoice from the Contractor. If the designated billing office fails to annotate the invoice with the date of receipt at the time of receipt, the invoice payment due date shall be the 10th day after the date of the Contractor's invoice; provided the Contractor submitted a proper invoice and no disagreement exists over quantity, quality, or Contractor compliance with contract requirements.

(ii) The 10th day after Government acceptance of supplies delivered or services performed by the Contractor.

(s) Order of precedence. Any inconsistencies in this solicitation or contract shall be resolved by giving precedence in the following order:

(1) The schedule of supplies/services.

(2) The Assignments, Disputes, Payments, Invoice, Other Compliances, Compliance with Laws Unique to Government Contracts, Unauthorized Obligations, and Commercial Supplier Agreements - Unenforceable Clauses paragraphs of this clause.

(3) The clause at 52.212-5.

(4) Addenda to this solicitation or contract, including any commercial supplier agreements as amended by the Commercial Supplier Agreements - Unenforceable Clauses provision.

(5) Solicitation provisions if this is a solicitation.

(6) Other paragraphs of this clause.

(7) The Standard Form 1449.

(8) Other documents, exhibits, and attachments.

(9) The specification.

(u) Unauthorized Obligations.

(1) Except as stated in paragraph (u)(2) of this clause, when any supply or service acquired under this contract is subject to any commercial supplier agreement (as defined in 502.101) that includes any language, provision, or clause requiring the Government to pay any future fees, penalties, interest, legal costs or to indemnify the Contractor or any person or entity for damages, costs, fees, or any other loss or liability that would create an Anti-Deficiency Act violation (31 U.S.C. 1341), the following shall govern:

(i) Any such language, provision, or clause is unenforceable against the Government.

(ii) Neither the Government nor any Government authorized end user shall be deemed to have agreed to such clause by virtue of it appearing in the commercial supplier agreement. If the commercial supplier agreement is invoked through an “I agree” click box or other comparable mechanism (e.g., “click-wrap” or “browse-wrap” agreements), execution does not bind the Government or any Government authorized end user to such clause.

(iii) Any such language, provision, or clause is deemed to be stricken from the commercial supplier agreement.

(2) Paragraph (u)(1) of this clause does not apply to indemnification or any other payment by the Government that is expressly authorized by statute and specifically authorized under applicable agency regulations and procedures.

(w) Commercial supplier agreements–unenforceable clauses. When any supply or service acquired under this contract is subject to a commercial supplier agreement (as defined in 502.101), the following language shall be deemed incorporated into the commercial supplier agreement. As used herein, "this agreement" means the commercial supplier agreement:

(1) Notwithstanding any other provision of this agreement, when the end user is an agency or instrumentality of the U.S. Government, the following shall apply:

(i) Applicability. This agreement is a part of a contract between the commercial supplier and the U.S. Government for the acquisition of the supply or service that necessitates a license or other similar legal instrument (including all contracts, task orders, and delivery orders under FAR Part 12).

(ii) End user. This agreement shall bind the ordering activity as end user but shall not operate to bind a Government employee or person acting on behalf of the Government in his or her personal capacity.

(iii) Law and disputes. This agreement is governed by Federal law.

(A) Any language purporting to subject the U.S. Government to the laws of a U.S. state, U.S. territory, district, or municipality, or a foreign nation, except where Federal law expressly provides for the application of such laws, is hereby deleted.

(B) Any language requiring dispute resolution in a specific forum or venue that is different from that prescribed by applicable Federal law is hereby deleted.

(C) Any language prescribing a different time period for bringing an action than that prescribed by applicable Federal law in relation to a dispute is hereby deleted.

(iv) Continued performance. The supplier or licensor shall not unilaterally revoke, terminate or suspend any rights granted to the Government except as allowed by this contract. If the supplier or licensor believes the ordering activity to be in breach of the agreement, it shall pursue its rights under the Contract Disputes Act or other applicable Federal statute while continuing performance as set forth in subparagraph (d) (Disputes).

(v) Arbitration; equitable or injunctive relief. In the event of a claim or dispute arising under or relating to this agreement, a binding arbitration shall not be used unless specifically authorized by agency guidance, and equitable or injunctive relief, including the award of attorney fees, costs or interest, may be awarded against the U.S. Government only when explicitly provided by statute (e.g., Prompt Payment Act or Equal Access to Justice Act).

(vi) Updating terms.

(A) After award, the contractor may unilaterally revise commercial supplier agreement terms if they are not material. A material change is defined as:

(1) Terms that change Government rights or obligations;

(2) Terms that increase Government prices;

(3) Terms that decrease overall level of service; or

(4) Terms that limit any other Government right addressed elsewhere in this contract.

(B) For revisions that will materially change the terms of the contract, the revised commercial supplier agreement must be incorporated into the contract using a bilateral modification.

(C) Any agreement terms or conditions unilaterally revised subsequent to award that are inconsistent with any material term or provision of this contract shall not be enforceable against the Government, and the Government shall not be deemed to have consented to them.

(vii) No automatic renewals. If any license or service tied to periodic payment is provided under this agreement (e.g., annual software maintenance or annual lease term), such license or service shall not renew automatically upon expiration of its current term without prior express consent by an authorized Government representative.

(viii) Indemnification. Any clause of this agreement requiring the commercial supplier or licensor to defend or indemnify the end user is hereby amended to provide that the U.S. Department of Justice has the sole right to represent the United States in any such action, in accordance with 28 U.S.C. 516.

(ix) Audits. Any clause of this agreement permitting the commercial supplier or licensor to audit the end user’s compliance with this agreement is hereby amended as follows:

(A) Discrepancies found in an audit may result in a charge by the commercial supplier or licensor to the ordering activity. Any resulting invoice must comply with the proper invoicing requirements specified in the underlying Government contract or order.

(B) This charge, if disputed by the ordering activity, will be resolved in accordance with subparagraph (d) (Disputes); no payment obligation shall arise on the part of the ordering activity until the conclusion of the dispute process.

(C) Any audit requested by the contractor will be performed at the contractor's expense, without reimbursement by the Government.

(x) Taxes or surcharges. Any taxes or surcharges which the commercial supplier or licensor seeks to pass along to the Government as end user will be governed by the terms of the underlying Government contract or order and, in any event, must be submitted to the Contracting Officer for a determination of applicability prior to invoicing unless specifically agreed to otherwise in the Government contract.

(xi) Non-assignment. This agreement may not be assigned, nor may any rights or obligations thereunder be delegated, without the Government's prior approval, except as expressly permitted under subparagraph (b) of this clause.

(xii) Confidential information. If this agreement includes a confidentiality clause, such clause is hereby amended to state that neither the agreement nor the contract price list, as applicable, shall be deemed "confidential information." Issues regarding release of "unit pricing" will be resolved consistent with the Freedom of Information Act. Notwithstanding anything in this agreement to the contrary, the Government may retain any confidential information as required by law, regulation or its internal document retention procedures for legal, regulatory or compliance purposes; provided, however, that all such retained confidential information will continue to be subject to the confidentiality obligations of this agreement.

(2) If any language, provision, or clause of this agreement conflicts or is inconsistent with the preceding paragraph (w)(1), the language, provisions, or clause of paragraph (w)(1) shall prevail to the extent of such inconsistency.

(End of clause)

I.4 HSAR CLAUSES INCORPORATED BY REFERENCE

The full text of a clause may be accessed electronically at HSAR website:

www.dhs.gov/publication/homeland-security-acquisition-regulation-deviations/

HSAR	TITLE	DATE
HSAR Class Deviation 15-01	Safeguarding of Sensitive Information	MAR 2015

J.1 LIST OF ATTACHMENTS

The following attachments are attached, either in full text or electronically at the end of the TOR.

ATTACHMENT	TITLE
A	COR Appointment Letter
B	Incremental Funding Chart (electronically attached .xls)
C	Draft Award Fee Determination Plan (AFDP)
D	Problem Notification Report (PNR) Template
E	Monthly Status Report (MSR) Template
F	Trip Report Template
G	Deliverable Acceptance-Rejection Report Template
H	CDM Dashboard Backlog (Refer to electronic Reading Room (eRR))
I	Department of Defense (DD) 254 (electronically attached .pdf)
J	Organizational Conflict of Interest (OCI) Statement
K	Corporate Non-Disclosure Agreement (NDA)
L	Travel Authorization Request (TAR) Template (electronically attached .xls)
M	Request to Initiate Purchase (RIP) Template (electronically attached .xls)
N	Consent to Purchase (CTP) Template (electronically attached .xls)
O	Removed at time of award
P	Removed at time of award
Q	Removed at time of award
R	Removed at time of award
S	CDM Federal Dashboard Concept of Operations (CONOPS) (July 2018)
T	Removed at time of award
U	Removed at time of award
V	Acquisition Risk Questions
W	Associate Contractor Agreement (ACA) Template
X	Reserved
Y	Reserved
Z	Analysis of Alternatives (AoA) Tracking Table
AA	Department of Defense (DD) 250 (electronically attached .pdf)
BB	CDM Program Test and Evaluation Master Plan (TEMP)
CC	CDM Technical Capabilities Requirements Documents, Volume 1 (electronically attached .pdf)

ATTACHMENT	TITLE
DD	CDM Technical Capabilities Requirements Documents, Volume 2 (electronically attached .pdf)
EE	Department of Defense (DD) 1149 (electronically attached .pdf)
FF	Program CDM Test Team Strategy for Solution Independent Verification and Validation (IV&V) ((electronically attached .pdf)
GG	Reserved
HH	CDM Dashboard Objectives
II	Procurement Report Template
JJ	Reserved
KK	CDM Dashboard SELC Process Overview
LL	CDM Dashboard Technical Demonstration
MM	Tier III Historical Data
NN	AWARE Technical Design Document
OO	AWARE Dashboard Requirements (Refer to eRR)
PP	CDM Logical Data Model Document (Refer to eRR)
QQ	CDM Task Order Group Solution Sets and Dashboard Status (Refer to eRR)

CLIN	CLIN TYPE	COST OVERRUN CEILING	ESTIMATED COST	ESTIMATED BASE FEE or FIXED FEE	ESTIMATED AWARD FEE	TOTAL ESTIMATED	FUNDED COST	FUNDED BASE FEE or FIXED FEE	FUNDED AWARD FEE	TOTAL FUNDED	ADD/REMOVE INCREMENTAL FUNDING	AMOUNT of LOST AWARD FEE	AMOUNT REMOVED from COST & BASE FEE FUNDING after POP (CPAF only)	ADD COST OVERRUN FUNDING	Base Fee/ Fixed Fee Actual %	Award Fee Actual	Total Fee %
0001	LABOR	(b) (4)													(b) (4)		
0004	LABOR																
0005	TRAVEL																
0006	ODCs																
0007	CAF																
SUB																	
1001	LABOR																
1002	LABOR																
1003	HOSTING																
1004	LABOR																
1005	TRAVEL																
1006	ODCs																
1007	CAF																
SUB																	
2001	LABOR																
2002	LABOR																
2003	HOSTING																
2004	LABOR																
2005	TRAVEL																
2006	ODCs																
2007	CAF																
SUB																	
3001	LABOR																
3002	LABOR																
3003	HOSTING																
3004	LABOR																
3005	TRAVEL																
3006	ODCs																
3007	CAF																
SUB																	
4001	LABOR																
4002	LABOR																
4003	HOSTING																
4004	LABOR																
4005	TRAVEL																
4006	ODCs																
4007	CAF																
SUB																	
5001	LABOR																
5002	LABOR																
5003	HOSTING																
5004	LABOR																
5005	TRAVEL																
5006	ODCs																
5007	CAF																
SUB																	
4008																	
TOTAL		(b) (4)				$ 276,112,559	$ (b) (4)	$ -	$ -	$ 7,733,568							

Note: The amounts in Columns Q - S represent the actual rate of fee and may appear to vary from negotiated rates due to:
---Facilities Capital Cost of Money (FCCoM)
---blended fee rates as a result of different fee on prime and sub costs

INSTRUCTIONS -- Fill in only the Columns/colors per instructions below. Do not change formulas in white cells. Gray cells are unused.

1 Columns D, E and F are filled in using dollar values from Section B CLINs (at award or from the revised contractor proposal that reflects any ceiling decreases, increases, or realignments). Please try to avoid use of cents in awards or funding.

2 Column L is used to obligate/deobligate incremental funding. Continue the formula to create a trail of funding actions.
---Changing numbers in this block will automatically adjust cost, base/fixed fee and award fee.
---Incremental Funding MUST be obligated/deobligated with proper proportions of cost and fee!

3 Column M is ONLY used to deobligate "lost" award fee. Continue the formula to create a trail of actions.
---Note that this amount WILL differ from the "lost" amount from the AFDP primarily driven by funding exceeding award fee allocation un
---These numbers should be entered as positive; example - enter 20,000 not -20,000

4 Column N is ONLY used to deobligate any excess **CPAF** Funded Cost and Base Fee after completion of the CLIN PoP.
---These numbers should be entered as positive; example - enter 20,000 not -20,000

5 Columns C and O are used for Cost Overrun (cost incurred above ceiling which receives NO fee).

6 Before each Modification, create a copy of the most current worksheet as a new Tab at the bottom of the worksheet. Complete your modification changes in the new Tab. DO NOT alter anything in the previous modification's worksheet.

7 Rename the new tab with the modification number, then input your changes to this new worksheet only.

8 Make sure that window in word document is displaying Columns A - K and all rows.

9 Do NOT delete any column or row because it will impact the formulas. If you must, right click the column and select hide to take the column out of view.